ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ
МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ (УНИВЕРСИТЕТ)
МИНИСТЕРСТВА ИНОСТРАННЫХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

На правах рукописи

Зиновьева Елена Сергеевна

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПРОБЛЕМЫ, СУБЪЕКТЫ, ПЕРСПЕКТИВЫ

Специальность 23.00.04 – Политические проблемы международных отношений, глобального и регионального развития

Диссертация на соискание ученой степени
доктора наук

Научный консультант
доктор исторических наук, профессор
Крутских А.В.

Москва – 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ..... 5

ГЛАВА 1. ВЛИЯНИЕ ИНФОРМАЦИОННОЙ РЕВОЛЮЦИИ НА МИРОВУЮ ПОЛИТИКУ 42

1.1. Научно-технологическое измерение мировой политики: теоретико-методологические основания анализа..... 42

1.1.1. Мирополитическая концептуализация научно-технологического развития 42

1.1.2. Теоретические основы анализа информационной революции в контексте международной политики и безопасности 49

1.2. Развитие информационного общества в контексте мировой политики..... 55

1.2.1. Интернет как основа информационного общества: тенденции развития 55

1.2.2. Регионализация глобального информационного пространства 61

1.2.3. Управление Интернетом в контексте международной безопасности ... 66

1.3. Политико-экономические аспекты глобальной информатизации 76

1.3.1. Влияние информационной революции на мировую экономику: политические аспекты 76

1.3.2. Интернет-компании как акторы мировой политики 83

ГЛАВА 2. МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА СОВРЕМЕННОМ ЭТАПЕ 94

2.1. Международная информационная безопасность: подходы к определению понятия 94

2.2. Субъекты и характер угроз международной информационной безопасности 106

2.3. Объекты международной информационной безопасности 120

2.3.1. Основные подходы к определению объектов международной информационной безопасности 120
2.3.2. Обеспечение безопасности критических информационных инфраструктур 123
2.3.3. Социальные медиа в контексте «цифровой дипломатии» и информационной безопасности 133
2.4. Политические проблемы применимости международного права к информационной сфере 158
ГЛАВА 3. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 170
3.1. Формирование международных режимов информационной безопасности на различных уровнях мировой политики 170
3.1.1. Глобальный уровень 171
3.1.2. Региональный уровень 184
3.1.3. Двусторонний уровень 200
3.1.4. Транснациональный уровень 203
3.2. Специфика международного сотрудничества по обеспечению информационной безопасности: сравнительный анализ 214
3.2.1. Формирование режима контроля над ядерными вооружениями: сопоставление с сотрудничеством по обеспечению информационной безопасности 215
3.2.2. Сравнение международного сотрудничества в сфере информационной безопасности с международно-правовым режимом космического пространства 225
3.3. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности 235
3.3.1. Позиции участников переговорного процесса и перспективы достижения глобального консенсуса по обеспечению информационной безопасности .. 235
3.3.2. Перспективы развития международного режима в сфере управления Интернетом 247

3.3.3. Направления адаптации международного права к информационной сфере 251
3.4. Информационная безопасность России в современных международных отношениях 257
ЗАКЛЮЧЕНИЕ 278
СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ 284
Приложения 328

ВВЕДЕНИЕ

Повсеместное распространение информационно-коммуникационных технологий (ИКТ) в экономике, политике, социальных отношениях создает потенциал развития, при этом порождая информационные вызовы и угрозы безопасности. Актуализируется проблема международной информационной безопасности, которая в силу транснационального характера информационной сферы не может быть разрешена на уровне отдельных государств и требует международных ответов. Международное взаимодействие, направленное на обеспечение информационной безопасности, находит свое отражение в деятельности таких международных организаций и форумов, как ООН, ОБСЕ, ШОС, ОДКБ, НАТО и ряд других.

Проблематика международной информационной безопасности привлекает в последние годы большое внимание как на экспертном, академическом, так и на политическом уровне. В настоящее время наметилось формирование глобального режима информационной безопасности, схожего с режимами, сложившимися в других высокотехнологичных областях мировой политики (космос и др.), но имеющего особенности, обусловленные как спецификой объекта регулирования, так и историей взаимодействия различных акторов в создании, развитии и регулировании глобального информационного пространства.

Россия, как и другие государства, осознает огромный потенциал информационно-коммуникационных технологий и опасность информационных вызовов и угроз, и активно продвигает на международной арене инициативы, направленные формирование международного режима информационной безопасности. Российская дипломатия инициативно участвует в международных переговорах в данной области, на практике реализуя официальную позицию,

изложенную в Концепции внешней политики России[1], а также в таких документах как Стратегия развития информационного общества[2], Доктрина информационной безопасности[3], в которых ставится задача обеспечить достойное место России как влиятельного центра силы в глобальном информационном обществе.

Значимость проблематики информационной безопасности для политики и дипломатии России подтверждается значительным числом инициатив в данной сфере. На международном уровне, к инициативам подобного рода следует отнести проект Концепции конвенции о международной информационной безопасности от 2011 г.[4], а также Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года[5], принятые в 2013 году. В 2011, а затем в 2015 году по инициативе Российской Федерации на рассмотрение ГА ООН был предоставлен документ Правила поведения в области международной информационной безопасности. На внутригосударственном уровне в 2015 году был принят Указ О некоторых вопросах информационной безопасности Российской Федерации, предполагающий создание в России государственного сегмента Интернета в целях обеспечения информационной безопасности[6]. В 2016 году была принята новая редакция Доктрины информационной безопасности Российской Федерации[7].

Обеспечение международной информационной безопасности тесно связано с процессами глобализации и регионализации, трансформацией государственного суверенитета и появлением новых форм международного сотрудничества и

---

[1] Концепция внешней политики Российской Федерации. Утверждена 30.11.2016. URL: http://www.scrf.gov.ru/documents/2/25.html

[2] 1. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. Утверждена указом Президента 09.05.2017. № 203. URL: http://kremlin.ru/acts/bank/41919

[3] Доктрина информационной безопасности от 5.12.2016. Утверждена указом Президента № 646. URL: http://www.scrf.gov.ru/documents/6/5.html

[4] Конвенция об обеспечении международной информационной безопасности (концепция). Утверждена 22.09.2011. URL: http://mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument

[5] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Утверждены Указом Президента 01.08.2013. № 1753

[6] О некоторых вопросах информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 22.05.2015 № 260. URL: http://www.rg.ru/2015/05/26/rosset-dok.html

[7] Доктрина информационной безопасности РФ. Утверждена указом Президента 5.12.2016№ 646. URL: http://www.scrf.gov.ru/documents/6/5.html

взаимодействия, а также важнейших проблем современных международных отношений, таких как обеспечение национальной и международной безопасности, проблема развития, обеспечения прав человека и др.

Актуальность темы настоящего исследования, следовательно, определяется как ее связью с актуальными проблемы современных международных отношений и внешней политики России, так и связью с актуальными вопросами современной науки о международных отношениях. Среди практического контекста проблематики международного сотрудничества в сфере информационной безопасности можно выделить:

- возрастающее значение информационной составляющей обеспечения национальной безопасности отдельных государств, а также международной безопасности;

- секьюритизацию глобального информационного пространства особенно после «дела Э. Сноудена»;

- угрозу милитаризации информационного пространства без выработанных при этом правил регулирования поведения государств в области международной информационной безопасности;

- сравнение некоторыми исследователями разрушительного потенциала информационного оружия с ядерным оружием[8];

- отсутствие государственной монополии легитимное насилие в сфере ИКТ, что вызвано не разработанностью правовой базы (в том числе на международном уровне) и сложностью классификации актов враждебного или злонамеренного использования ИКТ как насилия или агрессии.

В свою очередь научная актуальность исследуемой темы связана со следующими вопросами:

- анализ влияния Интернета на мировую политику (это один из шести наиболее важных вопросов современной теории международных отношений по версии Роберта Кохейна[9]);

---

[8] Актуальные военные аспекты обеспечения международной информационной безопасности / Под общ. ред С.В. Короткова. М.: Генеральный штаб ВС РФ, 2008. С. 16.

- исследование соотношения тенденций регионализации и глобализации в международном взаимодействии по обеспечению информационной безопасности;

- выявление специфики международного сотрудничества в сфере информационной безопасности по сравнению с другими высокотехнологичными областями мировой политики.

Объект исследования: информационная безопасность. **Предмет исследования**: международное сотрудничество по обеспечению информационной безопасности.

Цель исследования: выявить основные характеристики, природу и движущие силы международного сотрудничества по обеспечению информационной безопасности и определить особенности основных проблемных сфер международного сотрудничества, субъектов и перспектив взаимодействия в данной области.

Гипотеза исследования.

Гипотеза исследования основывается на теории международного сотрудничества как переговорного процесса, разрабатываемой такими авторами, как Дж. Фирон[10], Д. Панке[11], С. Розато[12] и др. Данная теория опровергает распространенное убеждение в научной литературе, что международное сотрудничество по каждой отдельной сфере (торговля, нераспространение, экология и т.п.) определяется особенностями стратегической структурой данной сферы. Согласно данному подходу сотрудничество во всех областях имеет одинаковую последовательность, состоящую из двух фаз: переговоры (bargaining) и принуждение к исполнению или реализация (enforcement).При этом в рамках диссертации данный подход рассматривается в более широком контексте теории международных режимов, которые, согласно подходу институционального торга О. Янга в ходе формирования проходят несколько стадий: определение повестки

---

[9] Keohane R. Big questions in the study of world politics // The Oxford Handbook of Political Science / Ed. by R. Goodin. Oxford University Press, 2009. P. 773

[10] Fearon J. D. Bargaining, enforcement, and international cooperation // International Organization. 1998. №. 02. P. 269-305.

[11] Panke D. Lock-in Strategies in International Negotiations: The Deconstruction of Bargaining Power //Millennium-Journal of International Studies. 2015. №. 2. P. 375-391.

[12] Rosato S. The Inscrutable Intentions of Great Powers //International Security. 2015. №. 3. P. 48-88.

дня; международные переговоры; операционализация достигнутых соглашений[13]. В настоящее время глобальный режим международной информационной безопасности находится на стадии определения повестки дня, в то время как отдельные региональные режимы находятся на стадии операционализации достигнутых соглашений.

Как правило, в работах реалистов акцент делался всегда на реализации. Эта часть сотрудничества описывается ими, как правило, с помощью модели дилеммы заключенного, которая показывает невозможность достижения оптимального результата в условиях структурной анархии. Без принуждения со стороны глобального суверена сотрудничество невозможно. Исключение составляет случаи гегемонстской стабильности. Либералы также делают акцент на реализационную части сотрудничества, но предлагают иную модель, которая допускает возможность сотрудничества даже при структурной анархии – стратегия «симметричного ответа», описанная Р. Аксельродом в «Эволюции сотрудничества». Условием сотрудничества при реализации данной стратегии является длина «тени будущего», т.е. значимость вопроса для акторов. Если акторы заинтересованы в сотрудничестве и не знают, когда их взаимодействие прекратится, при реализации стратегии «симметричного ответа», сотрудничество возникнет эволюционно.

Однако ни реалисты, ни либералы при анализе международного сотрудничества не уделяют необходимого внимания переговорной фазе, на которой определяются параметры договоров, а значит и меры, необходимые для их реализации. При этом переговорная фаза сотрудничества в рамках данного подхода Д. Фироном описывается моделью «войны на истощения». Если предмет сотрудничества для акторов представляет значительный интерес, то «война на истощение» будет длиться довольно долго и к фазе реализации акторы могут и не перейти. Иными словами, чем длиннее «тень будущего» от предмета переговоров (т.е. чем значимее обсуждаемый вопрос для акторов), тем меньше вероятности заключения работающей договоренности. Однако, если такая договоренность все

[13] Young O. R. Creating regimes: Arctic accords and international governance. Cornell University Press, 1998.P. 7.

же будет достигнута, то, учитывая высокую заинтересованность акторов, в ее реализации проблем быть не должно.

Значимость для акторов предмета сотрудничества	Фазы сотрудничества	
	Переговоры	Реализация
Высокая	Трудные	Легкая
Низкая	Легкие	Трудная

Отталкиваясь от модели международного сотрудничества Фирона, а также исходя из высокой значимости информационной безопасности для международного сообщества в целом и для его лидеров в частности, можно сформулировать следующую гипотезу: переговорная фаза сотрудничества будет длиться крайне долго и к фазе реализации оно может и не прийти. Однако, опираясь на логику реалистов, можно предположить, что условием перехода переговорной фазы к реализации может быть достижение между основными участниками переговоров (США, Россия и Китай) в сфере информационной безопасности зафиксированного паритета в возможности причинить друг другу взаимный неприемлемый ущерб. История развития международных отношений в ядерной сфере говорит в пользу такого предположения. Пока между двумя полюсами силы не установилось равновесие страха, сторонами безуспешно предлагались проекты по ограничению ядерного распространения или отказу от ЯО (план Баруха). После осознания равновесия страха стороны перешли к созданию режима и его имплементации, заключив договоренности об ограничении и сокращении ЯО, при этом реализация данных соглашений была эффективной. Альтернативным примером является международное взаимодействие по вопросам освоения околоземного космического пространства – США и СССР удалось достаточно быстро согласовать Договор о космосе 1967 года, в виду того, что практическое использование космического пространства, достижение стратегического превосходства в данной сфере и распространение на него государственного суверенитета ограничивалось текущим уровнем развития

технологий, однако имплементация настоящего соглашения (и ряда соглашений, последовавших за ним) осложняется желанием государств добиться превосходства в космосе, что в свою очередь способствует милитаризации космического пространства и дальнейшему развитию технологий использования космического пространства в военных целях в обход выше обозначенных соглашений[14].

Длительная переговорная фаза международного сотрудничества будет, скорее всего, маскировать гонку вооружений в информационной сфере пока острый международный кризис с применением информационного оружия не установит равновесие страха (баланс угроз в терминологии С. Уолта[15]) между сторонами и международное сотрудничество перейдет к фазе реализации, которая, учитывая значимость данного вопроса, обещает быть эффективной.

Проверка указанной гипотезы предполагает реализацию следующих задач.

Задачи исследования:

1. Оценить значимость информационно-коммуникационной сферы для мировой политики
    a. Определить влияние информационной революции на мировую политику и охарактеризовать подходы к исследованию данной проблематики.
    b. Выделить характеристики современного этапа развития сети Интернет других ИКТ как основы информационной революции.
    c. Провести анализ современных политических теорий информационного общества.
    d. Обосновать существование признаков регионализации глобального информационного пространства.
    e. Рассмотреть политико-экономические аспекты глобальной информатизации с целью определения особенностей политического влияния информационной революции на мировую экономику.

[14] Космос: оружие, дипломатия, безопасность / под ред. А. Арбатова, В. Дворкина. М., 2009. С. 91.
[15] Walt S. The progressive power of realism //American Political Science Review. 1997. № 4. P. 931-935.

2. Рассмотреть проблему управления Интернетом как вопрос международной безопасности.
3. Проанализировать существующие подходы к определению международной информационной безопасности и вычленить их сущностные характеристики.
4. Выделить субъекты и характер угроз международной информационной безопасности .
5. Выделить ключевые объекты международной информационной безопасности, особенно безопасность критических информационных инфраструктур.
6. Выделить политические аспекты проблемы применимости международного права к информационной сфере.
7. Проследить основные направления международного сотрудничества по обеспечению информационной безопасности на различном уровне (глобальный, региональный, двусторонний).
8. С помощью сравнительного анализа международного сотрудничества в сфере информационной безопасности, нераспространения ЯО, а также космической политики и дипломатии выявить специфику сотрудничества в сфере международной информационной безопасности по сравнению с другими областями международной политики, в том числе высокотехнологичными.
9. Определить перспективные тенденции формирования международного режима по обеспечению информационной безопасности.
10. Выявить интересы России в области информационной безопасности и управления Интернетом; сформулировать рекомендации по их продвижению в рамках международного сотрудничества.

Теоретико-методологическая база исследования

Методологической основой работы выступает системный подход, предполагающий рассмотрение современной мировой политики в качестве сложной системы различных взаимодействующих между собой акторов, как государственных, так и негосударственных. Он дает возможность выявить общие и специфические черты объекта и предмета исследования, тенденции и

качественные характеристики его развития. При этом автор придерживается позиции реализма при изучении позиций и интересов влиятельных государств в области информационной безопасности. К исследованию международного взаимодействия государств также был применен реалистский подход как парадигма анализа международных отношений в области обеспечения информационной безопасности. В то же время, акцент на силовом характере международных отношений, характерный для реалистов, не был абсолютизирован, ценности и идеалы также учитывались при анализе интересов государств в области международной информационной безопасности.

При исследовании международного сотрудничества по обеспечению информационной безопасности также были использованы теории среднего уровня – теория международных режимов, теория анализа переговорного процесса (bargaining) и теория секьюритизации.

При анализе процессов международного сотрудничества по обеспечению информационной безопасности автор использует положения теории международных режимов, разработанной такими авторами как Ст. Краснер, Р. Кохейн, Дж. Рагги и др[16]. Ст. Краснер определяет международные режимы как набор принципов, норм, правил и процедур принятия решений, вокруг которых сходятся ожидания акторов в данной области международных отношений[17].Согласно подходу С. Краснера, принципы отражают специфику сферы международной политики, на управление которой направлен режим. Нормы определяют права и обязательства участников режима и логически вытекают из принципов. Правила понимаются как применение принципов и норм международного режима. Процедуры принятия решений являются практическим воплощением основных элементов режима во внешней политике участников.

[16] Krasner S. Structural causes and regime consequence: regimes as intervening variables. // International Regimes. / Ed. by Krasner S. Ithaca, 1983 P. 1-21; Keohane R. O. The demand for international regimes //International organization. 1982. T. 36. №. 02. P. 325-355; Ruggie J. G. International regimes, transactions, and change: embedded liberalism in the postwar economic order //International organization. 1982. T. 36. №. 02. P. 379-415.

[17] Krasner S. Structural causes and regime consequence: regimes as intervening variables. // International Regimes. / Ed. by Krasner S. Ithaca, 1983.P. 2.

Достоинством данного подхода является его гибкость, так как режим не обязательно предполагает создание формальной международной организации, режимы могут быть неформальными и основанными на совпадающих ожиданиях участвующих государств относительно поведения в определенной области международной политики. Следует подчеркнуть кооперативную основу международных режимов, которые основаны на сотрудничестве, а не принуждении или навязывании определенных норм акторами, которые в этом заинтересованы. При этом автор опирался на подход институционального торга О. Янга в теории международных режимов, который выделяет три стадии, которые каждый режим проходит при формировании: определение повестки дня, переговоры и реализация достигнутых соглашений[18].

Для анализа переговорного процесса была использована теория международного сотрудничества как взаимоотношений в рамках модели «торга», разрабатываемая такими авторами, как Дж. Фирон[19], Д. Панке[20], С. Розато[21] и др. Согласно данному подходу сотрудничество во всех областях имеет одинаковую последовательность, состоящую из двух фаз: переговоры (bargaining) и принуждение к исполнению или реализация (enforcement). При этом переговорная фаза сотрудничества в рамках данного подхода описывается моделью «войны на истощения». Если предмет сотрудничества для акторов представляет значительный интерес, то «война на истощение» будет длиться довольно долго и к фазе реализации акторы могут и не перейти. Однако в условиях, когда участники переговоров ощущают взаимную уязвимость, вероятность достижения эффективных договоренностей существенно возрастает.

Подход институционального торга О. Янга и концепция Д. Фирона схожим образом понимают логику международного взаимодействия, и их совместное использование позволяет, с одной стороны детально проанализировать

[18] . Young O. International Cooperation: Building Regimes for Natural Resources and the Environment. Ithaca, 1989 251 p.
[19] Fearon J. D. Bargaining, enforcement, and international cooperation // International Organization. 1998. №. 02. P. 269-305.
[20] Panke D. Lock-in Strategies in International Negotiations: The Deconstruction of Bargaining Power //Millennium-Journal of International Studies. – 2015. №. 2. P. 375-391.
[21] Rosato S. The Inscrutable Intentions of Great Powers //International Security. 2015. №. 3. P. 48-88.

международное сотрудничество по обеспечению информационной безопасности в различных регионах, а также провести анализ международного взаимодействия в других высокотехнологичных секьюритизированных областях мировой политики (контроль над ядерными вооружениями и освоение космического пространства) на основании модели О. Янга, а с другой – сделать прогнозы на основании анализа стратегической структуры отношений между наиболее влиятельными акторами в рамках режима международной информационной безопасности.

Теория секьюритизации Копенгагенской школы была использована с целью анализа формирования повестки дня международного сотрудничества по обеспечению информационной безопасности. Среди представителей теории секьюритизации следует назвать Б. Бузана, О. Уивера, Я. Вилде[22]. Согласно теории секьюритизации проблема рассматривается как угроза безопасности в том случае, если она представляется как угрожающая выживанию определенного референтного объекта (как правило, в качестве референтного объекта выступает государство, включая правительство, территорию и общество). Особый характер проблем безопасности обосновывает использование экстраординарных средств для их разрешения, легитимируя использование военной силы, а в более широком смысле открывая для государства возможность мобилизовать или привлекать особые силы и средства[23].

Выделяют следующие категории, используемые при анализе секьюритизированных проблем:

1. Референтный объект – сфера действительности, которая находится в состоянии экзистенциальной угрозы и которая обладает легитимным правом на выживание;

2. Секьюритизирующие акторы – акторы, которые секьюритизируют проблемы, указывая на наличие экзистенциальной угрозы по отношению к данной проблеме;

[22] Buzan B., Wæver O., De Wilde J. Security: a new framework for analysis. Lynne Rienner Publishers, 1998.241 p.
[23] Там же. P. 21.

3. Функциональные акторы –акторы, которые имеют возможность оказывать влияние на динамику развития секьюритизируемой области, не являясь секьюритизирующими акторами (напрямую определяющими референтный объект как находящийся под угрозой выживания), они, тем не менее, имеют возможность оказывать влияние на процесс принятие решений в сфере безопасности[24].

Согласно Копенгагенской школе, процесс секьюритизации состоит из двух этапов: политизация проблемы (возведение ее в сферу публичной политики как требующую решения правительства или, более редко, некоторых других форм общего руководства) и секьюритизация проблемы (возведенеие проблемы в ранг угроз безопасности, требующих принятия чрезвычайных мер, выходящих за рамки стандартных политических процедур государства)[25].Концепция секьюритизации позволила проанализировать процесс формирования повестки дня, внешнеполитический и исследовательский дискурс в области международной информационной и кибер безопасности.

Из методов специальных наук особое внимание было уделено историко-описательному и политико-описательному методам, обеспечившим систематизацию и общий анализ фактологической информации, а также сравнительно-историческому методу. Историко-описательный метод оказался полезным для изучения эволюции процесса международного сотрудничества в области информационной безопасности. Сравнительно-исторический метод позволил провести сравнительный анализ развития международных режимов в высокотехнологичных областях мировой политики.

Для анализа конкретных примеров, иллюстрирующих выдвигаемые в работе положения теоретического характера, применен подход “case-study”[26]. С позиций данной теории кейс международного сотрудничества в сфере информационной безопасности представляет собой отклоняющийся кейс, так как теоретики информационного общества рассматривают взаимодействие в данной области как принципиально отличающееся от других областей международной

[24]Там же. P. 36.
[25]Там же. P. 23.
[26] Gerring J. Case study research: principles and practices. Cambridge University Press, 2006. 271 p.

политики[27]. Настоящая работа показывает, что взаимодействие в области международной безопасности соответствует общей логике международного сотрудничества в условиях анархии, и таким образом, вносит вклад в развитие теории информационного общества и концептуализацию взаимного влияния науки и технологий и мировой политики. Исследование кейса международной информационной безопасности дополнено изучением международного взаимодействия в таких высокотехнологичных и секьюритизированных областях, как контроль над ядерными вооружениями и международное взаимодействие по вопросам освоения космического пространства.

Степень научной разработанности проблемы. Для анализа сложившейся ситуации в сфере международной информационной безопасности, а также исследования международного сотрудничества в данной области, потребовалось знакомство с несколькими большими пластами литературы.

Международное взаимодействие по обеспечению информационной безопасности проходит на фоне процессов глобализации, углубления внутрирегионального взаимодействия и сопутствующей этим процессам фрагментации и разобщения. Для лучшего понимания изменяющейся природы международной среды, в рамках которой протекает взаимодействие по обеспечению информационной безопасности, необходимо было изучить работы, посвященные исследованию современного состояния международной системы. Среди российских исследователей, занимающихся исследованием современного состояния международных отношений и мировой политики в самом широком понимании, следует отметить: Богатурова А.Д., Воскресенского А.Д., Косолапова Н.А., Лебедеву М.М., Мельвиля А.Ю., Хрусталева М.А.[28]. Видными зарубежными

[27] См. напр.: Курбалиа Й. Управление Интернетом / пер. с англ. М.: Координационный центр национального домена сети Интернет, 2010 208 с.; Chadwick A., Howard P. Routledge Handbook of Internet Politics. Taylor&Francis, 2008.511 p.; Choucri N. Cyberpolitics in International Relations. MIT Press, 2012.311 p. и др.

[28] Богатуров А.Д. Очерки теории и политического анализа международных отношений. / Богатуров А.Д., Косолапов Н.А., Хрусталев М.А. М.:НОФМО, 2002.309 с.; Мельвиль А.Ю. Пространство и время в мировой политике // Космополис. 2007. №2 (18). С. 117-122; Хрусталев М.А. Анализ международных ситуаций и политическая экспертиза. Очерки теории и методологии М.:НОФМО, 2008. 232 с.; Лебедева М.М. Мировая

учеными, исследующими эти вопросы, являются И. Валлерстайн, А. Вендт, Д. Най, Р. Кохейн, К. Уолц, Д. Миршаймер и другие[29]. Все вышеперечисленные исследователи являются учеными высокого концептуального уровня, и их работы составили основу методологического аппарата исследования.

В качестве теоретической парадигмы при исследовании международной политики в сфере информационной безопасности была использования школа политического реализма в теории международных отношений. Представители политического реализма анализируют внешнюю политику государств, так же как и международные отношения в целом, с позиций стремления государств к обеспечению национальной безопасности за счет усиления собственной власти и влияния, при этом единственным регулятором международного взаимодействия выступают сила и баланс сил. К представителям реализма в истории философской и исторической мысли, заложившим основу для данного направления в теории международных отношений, можно отнести Фукидида, Т. Гоббса, Н. Маккиавелли, К. фон Клаузевица. Школа политического реализма представлена именами Р. Гилпина, Дж. Гриеко, Дж. Миршаймера, Д. Снидала[30]. Особое влияние на концептуальный аппарат настоящей работы оказала теория баланса угроз С. Уолта[31].

Международное сотрудничество в области информационной безопасности было проанализировано с позиций теории международных режимов. Теория режимов представляет собой одно из авторитетных теоретических направлений исследования международного сотрудничества, сохраняя свое влияние вот уже в

политика. М.: Аспект-Пресс, 2013. 256 с.; Воскресенский А.Д. Мировое комплексное регионоведение и перспективы построения незападной (китаизированной) теории международных отношений // Полис. Политические исследования. 2013. № 6. С. 82-96

[29]Валлерстайн И. Анализ мировых систем и ситуация в современном мире - СПб.: Университетская книга, 2001; Wendt A. Constructing International Politics //InternationalSecurity.1995. № 1(20). P. 71-81; Wendt A. Constructing International Politics // International Security. 1995. № 1(20). P. 71-81; Waltz K. N. Theory of international politics. Waveland Press, 2010; Keohane R. O., Nye Jr J. S. Power and interdependence in the information age //Foreign affairs. 1998. P. 81-94.; Keohane R. O. After hegemony: Cooperation and discord in the world political economy. – Princeton University Press, 2005.; Mearsheimer J. The tragedy of great power politics. WW Norton & Company, 2001. 592 p.

[30] Gilpin R. War and change in world politics. Cambridge University Press, 1983; Grieco J. M. Anarchy and the limits of cooperation: a realist critique of the newest liberal institutionalism //International organization. 1988. №. 03. P. 485-507; Mearsheimer J. J. The tragedy of great power politics. WW Norton & Company, 2001 592 p.; Snidal D. Relative Gains and the Pattern of International Cooperation //American Political Science Review. 1991. №. 03. P. 701-726.

[31] Walt S. M. Alliance formation and the balance of world power //International security. 1985. № 4. P. 3-43.

течение трех десятилетий. Данная теория позволяет комплексно описать и проанализировать сложившуюся ситуацию в области международного сотрудничества по информационной безопасности, и более того, сделать прогнозы и дать рекомендации. Кроме того, теория международных режимов обладает методологическим аппаратом анализа переговорного процесса.

Среди высокоцитируемых авторов, работающих в рамках теории международных режимов, могут быть отмечены Р. Аксерольд, Р. Кохейн, Ст. Краснер, Ф. Краточвил, Дж. Миршаймер, Дж. Най, Дж. Рагги, А. Стейн, Э. Хаас, О. Янг, и др[32]. В российской науке проблемами международных режимов безопасности занимаются проф. Петровский В.Е.[33] и ряд других исследователей. Обобщением различных направлений теории режимов занимался авторский коллектив под руководством А.Хансклейнера, выделивший три направления теории режимов: реалистское, либеральное и конструктивистсткое[34].

Исследования переговорного процесса в ходе формирования международных режимов по обеспечению информационной безопасности были проведены в рамках теории переговорного торга (bargaining), разрабатываемой Дж. Фирон[35], Д. Панке[36], С. Розато[37].

---

[32] Axelrod R. The evolution of cooperation. -New York, 1984; Axelrod R., Keohane R. Achieving Cooperation Under Anarchy: Strategies and Institutions. // Neorealism and neoliberalism: the contemporary debate / ed. by Baldwin D. New York, 1993; Keohane R., Nye J. Power and Interdependence: World Politics in Transition. Boston. 1989; Keohane R. After Hegemony – Cooperation and Discord in the World Political Economy. Princeton, 1984; Keohane R. International Institutions and State Power: Essays in International Relations Theory. Boulder, 1989; Krasner S. International regimes. Ithaca, 1983; Kratochwil F., Ruggie J. International Organization: A State of the Art and an Art of the State// International Organization, 1986. No. 40 (4). P. 753–775. Mearsheimer J. The False Promise of International Institutions // International Security. 1994. No. 15 (3). P. 5–49. Ruggie G. International regimes, transactions and change: embedded liberalism in the postwar economic order // International Regimes. / Edited by Krasner S. Ithaca, 1983; Stein A. Coordination and Collaboration: regimes in an Anarchic World. // International Organization. No. 2. P. 299-324; Haas P. Epistemic Communities and International-Policy Coordination Introduction. // International Organization 1992. No. 46 (1) P. 1-35; Young O. International Cooperation: Building Regimes for Natural Resources and the Environment. Ithaca, 1989; Young O. Regime dynamic. The rise and fall of international regimes // International Relations. Critical concepts in political science. Vol. 2. / Edited by Linklater A. London, 2004; Levy M., Young O., Zuern M. The study of international regimes // European Journal of International Relations. 1995. № 3(1). P. 267-330.

[33]Петровский В.Е. Азиатско-тихоокеанские режимы безопасности после «холодной войны»: эволюция, перспективы российского участия. М, 1998

[34] Hasenclever A., Mayer P., Rittberger V. Theories of International Regimes. - New York, 1997; Hasenclever A., Mayer P., Rittberger V. Integrating theories of international regimes // Review of International Studies. 2000. No. 26. P. 3–33.; Levy M, Young O, Zuern M. The study of international regimes // European Journal of International Relations. 1995. № 3(1). P. 267-330.

[35] Fearon J. D. Bargaining, enforcement, and international cooperation // International Organization. 1998. №. 02. P. 269-305.

[36] Panke D. Lock-in Strategies in International Negotiations: The Deconstruction of Bargaining Power //Millennium-Journal of International Studies. 2015. №. 2. P. 375-391.

При анализе внешнеполитического и исследовательского дискурса в сфере международной информационной безопасности была использования концепция секьюритизации Копенгагенской школы, наиболее видными представителями которой являются Б. Бузан, О. Уивер, Я. Вилде[38].

В ходе анализа механизмов и инструментов обеспечения международной информационной безопасности, автор опирался на исследования, посвященные историческому развитию и современному состоянию международного телекоммуникационного режима[39], а также особенностям регулирования информационно-коммуникационных технологий в исторической ретроспективе, подготовленные такими авторами как В. Дрейк, Т. Кертис, С. Сиохру, М. Захер и Б. Саттон[40].

Международное взаимодействие в области обеспечения информационной безопасности было исследовано в сопоставлении с международной политикой в таких областях, как космическая политика, а также нераспространение ядерного оружия.

Среди работ, изучающих международную космическую политику, следует отметить работы таких авторов как Арбатов А.Г., Дворкин В.З., Фененко А.В., Роговский Е.А. [41], а также зарубежных авторов, в том числе Н. Борманн, М. Шихан, Н. Танненвальд[42] и др.

---

[37] Rosato S. The Inscrutable Intentions of Great Powers //International Security. 2015. №. 3. P. 48-88.

[38] Buzan B., Wæver O., De Wilde J. Security: a new framework for analysis. Lynne Rienner Publishers, 1998.

[39] Под международным телекоммуникационным режимом понимается международный режим (в соответствии с определением С. Краснера), регулирующий международное взаимодействие по регулированию телекоммуникационной индустрии и использования телекоммуникаций гражданами государств (под телекоммуникациями понимается комплекс технических средств для передачи информации на расстояние, в т.ч. телеграф, телефонная связь, радио связь, сотовая связь, электросвязь и др.).

[40] Drake W. The rise and decline of the international telecommunication regime. // Regulating global information society. / Ed. by Masrsden Ch. London: Routledge, 2000. – P. 124-178; Curtis T. The international telecommunication regimes in the information age. // Prometheus. 2003. No 4 (21). P. 399-414; Chun W., Keenan T. New media, old media: a history and theory reader. London: Routledge, 2006; Siochru S. Global Media Governance: A Beginner s Guide. / Siochru S., Girard B., Mahan A. Lanham: Rowman & Littlefield, 2002; Zacher M., Sutton B. Governing global networks: international regimes for transportation and communication. NY: Cambridge University Press, 1996.

[41] Космос: оружие, дипломатия, безопасность / под ред. А. Арбатова, В. Дворкина. М., 2009; Фененко А.В. Конкуренция в космосе и международная безопасность// Международные процессы. 2008 Том 6. №3 (18); Фененко А. Международное соперничество за освоение общих пространств // Международные процессы. 2010. Январь – апрель. Т. 8, № 1 (22). С. 14–30; Роговский Е.А. Информационные аспекты космической политики США// Россия и Америка в XXI веке. 2008. №3. URL: http://www.rusus.ru/?act=read&id=984

[42] Securing Outer Space: International Relations Theory and the Politics of Space / Ed by Bormann N., Sheehan M. Routledge, 2009; Tannenwald N. Law versus power on the high frontier: The case for a rule-based regime for outer space //Yale Journal on International Law. 2004. URL: http://drum.lib.umd.edu/bitstream/1903/7902/1/tannenwald.pdf

При анализе международного режима контроля над ядерными вооружениями были использованы работы таких авторов, как Арбатов Г.А., Дворкин В.З., Кокошин А.А., Рогов С.М., Сафранчук И.А.[43], а также зарубежных авторов, в том числе П. Гольдшмидт, Дж. Эктон[44].

В ходе исследования международной информационной безопасности необходимо было, прежде всего, рассмотреть основные направления исследования глобального информационного общества. Теоретические аспекты развития информационного общества проработаны в трудах российских авторов, в том числе Иноземцева В.Л., Чугунова А.В., Паршина П.Б., Сурмы И.В.[45], а также зарубежных авторов Д. Белла, Э. Тоффлера, М. Кастелльса, Ф. Уэбстера и др[46]. По этой тематике также были защищены диссертационные исследования, подроговленные российскими авторами Буряковой О.С., Мелюхиным И.С.[47] и др.

Немало внимания в последние политологи и специалисты в области международных отношений уделяют и последствиям формирования информационного общества для международных отношений и мировой политики. Из российских авторов эта проблематика изучалась, в частности, Балуевым Д.Г.,

---

[43] Ядерное сдерживание и нераспространение /Под ред. А. Арбатова и В. Дворкина. М.: Московский Центр Карнеги, 2005; Кокошин А.А. Ядерные конфликты в XXI веке (типы, формы, возможные участники). М.: «Медиа-Пресс», 2003; Сафранчук И.А. Режим нераспространения ядерного оружия // Современные глобальные проблемы мировой политики. / Под ред. М.М. Лебедевой. С. 127-139; Сафранчук И.А. Сохранится ли запрет на ядерные испытания // Россия в глобальной политике. 2006. № 3. URL: http://globalaffairs.ru/number/n_6812; Белоус В.С., Сафранчук И.А. Безопасность и надежность ядерных аресеналов без испытаний. Доклад российского представительства Центра оборонной информации. М.: Воениздат, 2006.

[44] Acton J. M. the Problem with nuclear Mindreading //Survival. 2009. №. 1. P. 119-142; Goldschmidt P. The Urgent Need to Strengthen the Nuclear Non-Proliferation Regime //Policy Outlook. 2006. №. 25. P. 360.

[45] Иноземцев В.Л. Современное постиндустриальное общество: природа, противоречия, перспективы. М.: Логос, 2000; Паршин П.А. Глобальное информационное общество и мировая политика / П.Б. Паршин // Аналитические доклады Института международных исследований МГИМО (У) МИД России. 2009. №2(23). С.3-37; Чугунов А.В. Развитие информационного общества: теории, концепции и программы: Учебное пособие. - СПб.: Ф-т филологии и искусств СПбГУ, 2007; Сурма И.В. Глобальный наднациональный актор международных отношений и его социальная философия // Вестник МГИМО-Университета. 2013. № 4. URL: http://www.vestnik.mgimo.ru/razdely/mirovaya-politika/globalnyy-nadnacionalnyy-aktor-mezhdunarodnyh-otnosheniy-i-ego-socialnaya

[46] Castells M. Communication, Power and Counter-power in the Network Society // International Journal of Communication. – 2007. № 1.P. 238-266; Castells M. The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance // The Annals of the American Academy of Political and Social Science. 2008. № 616. URL:http://prtheories.pbworks.com/w/file/fetch/45138545/Castells_2008_The_New_Public_Sphere.pdf; Toffler A. Powershift: Knowledge, Wealth, and Violence in the 21st Century. N.Y.: BantamBooks, 1990 640 p.; Белл Д. Грядущее постиндустриальное общество: опыт социального прогнозирования: пер. с англ. М.: Academia, 1999. 320 с.; Уэбстер Ф. Теории информационного общества: пер. с англ. М.: Аспект-Пресс, 2004. 400 с.

[47] Бурякова О.С. Информационная и знаниевая революции: сравнительный анализ концепций. Дисс ... кандидата филос. наук. Ростов-на-Дону, 2011; Мелюхин И.С. Информационное общество: проблемы становления и развития (философский анализ). Дисс... доктора полит.наук. М., 1997.

Песковым Д.Н., Панцеревым К.А., Смирновым А.И.[48]За рубежом международно-политические аспекты развития новых информационных технологий нашли отражение в работах таких известных специалистов по мировой политике, как Р. Кохэн, Д. Най, Дж. Мэтьюс, Дж. Розенау, Д. Роткопф, С. Сассен, и множества других авторов (в т. ч. Ч. Лэнгдона, Д. Паппа и Д. Элбертса, У. Ристона, К. Роджерсона, С. Шварцстайна, М. Прайса)[49].

Особенности ИКТ и актуальные тенденции их развития с политологической точки зрения исследуют такие зарубежные авторы как М. Кастельс, К. Кукьер и В. Майер-Шедбергер[50]. Вопросам роли социальных сетей и новых медиа и государственной политике, безопасности и дипломатии посвящают свои исследования такие авторы как Ширин С.С., Демидов О.В., Цветкова Н.А.[51]; среди зарубежных исследователей этой проблематикой занимаются В. Ван Донк, Б. Лоадер, П. Никсон, Д. Рахт, Д. Дрезнер, Х. Фарелл, С. Эдай[52]. Политико-экономическое измерение процессов глобальной информатизации анализируют

[48] Балуев Д.Г. Информационная революция и современные международные отношения Нижний Новгород, 2001. 108 с.; Песков Д.Н. Интернет в мировой политике: формы и вызовы // Современные международные отношения и мировая политика / Отв. ред. А.В. Торкунов; МГИМО(У) МИД России. М.: Просвещение, 2004. С. 155-172; Смирнов А.И. Мегатренды цифровой эпохи//Глобальная безопасность в цифровую эпоху: стратагемы для России / Под ред. А.И.Смирнова. М.: ВНИИ Геосистем, 2014.

[49] Keohane R., Nye J. Power and Interdependence in the Information Age // Foreign Affairs. 1998. No. 5. P. 81-94; Nye J, Owens W. America's Information Edge // Foreign Affairs. 1996. P. 20-36; Rogerson K. Information interdependence: Keohane and Nye's complex interdependence in the information age // Communication & Society. 2000. Vol. 3. Issue 3.P. 415-436; Rosenau J. States, Sovereignty, and Diplomacy in the Information Age. Paper prepared for presentation at the Panel on «Virtual Diplomacy: A Revolution in Diplomatic Affairs Theory, Annual Meeting of the International Studies Association. Washington, D.C., 1998.URL http://www.usip.org/virtualdiplomacy/publications/reports/jrosenauisa99.html; Rothkopf D. Cyberpolitik: the changing nature of power in the information age // Journal of International Affairs. 1998. No. 2.P. 325-359; Schwartzstein S. The Impact of Information Revolution on International Relations // IPTS Report. 1996. Vol 06. URL: http://www.jrc.es/pages/iptsreport/vol06/english/art-it2.htm; Tehranian M. Global Communication and World Politics: Domination, Development, and Discourse. Boulder: Lynne Rienner, 1999; Wenger A. The Internet and the Changing Face of International Relations and Security// Information & Security. 2001. Volume 7. P. 5-11.

[50] Castells M. The Rise of the Network Society: The Information Age: Economy, Society, and Culture. JohnWiley&Sons, 2011; Кукиер К., Майер-Шёнбергер В. Большие данные // Россия в глобальной политике. 2013. № 3. URL: http://www.globalaffairs.ru/number/Bolshie-dannye--16038

[51] Демидов О.В. Социальные сетевые сервисы в контексте международной и национальной безопасности //Индекс безопасности. 2013. №. 1. С. 100-122; Цветкова Н.А. Программы Web 2.0 в публичной дипломатии США // США и Канада: Экономика, политика, культура. 2011. №3. С. 109-122; Ширин С.С. Сообщества разработчиков Интернет-проектов // Вестник МГИМО – Университета. 2014. № 6. URL: http://vestnik.mgimo.ru/sites/default/files/pdf/09mir_politika_shirin.pdf

[52] Drezner D. W., Farrell H. Introduction: Blogs, politics and power: a special issue of Public Choice //Public Choice. 2008. №. 1-2. P. 1-13; Aday S. Blogs and bullets. New media in contentious politics // United States Institute of Peace. August 2010. №5. URL:http://www.newmediacenter.ru/wp-content/uploads/2011/10/adayetal2010.pdf; Cyberprotest: new media, citizens and social movements / Ed. By W. van d Donk, B. Loader, P. Nixon, D. Rucht. Routlege, 2004.

по большей части западные исследователи, в том числе Д. Най, М. Кастельс, С. Фьюкс[53].

Особо следует отметить работы, анализирующие процессы глобальной информатизации с правовой точки зрения. На сегодняшний день написано особенно много работ, посвященных правовому регулированию использования ИКТ, сформировалась даже отдельная отрасль права – информационное право. Среди наиболее известных российских, работающих в этом направлении исследований, авторов следует назвать Бачило И.Л., Наумова В. Б., Серго А. Г.[54]; среди зарубежных – М. Фрумкина, Д. Курбалиа, Д. Ментэ, и др.[55]Среди классических трудов в данной области необходимо назвать работы авторитетного исследователя Л. Лессига, который впервые предположил, что в Интернет-пространстве помимо традиционных юридических инструментов регулирования, управляющую функцию выполняют также программные средства[56]. При этом в последние годы появляются работы, посвященные также такой актуальной проблемы информационной безопасности, как применимость международного права к информационной сфере в контексте обеспечения безопасности, в том числе Таллинское руководство, подготовленное центром Исследования и мониторинга кибер-угроз НАТО[57], а также работы таких авторов, как А.В.

---

[53] Fuchs C. Dallas Smythe Reloaded: Critical Media and Communication Studies Today. // The audience of commodity in digital age. / Ed. by McGuigan L., Manzerolle V. New York: Peter Lang, 2013; 175. Nye J. The Future of Power in the 21st Century, N.Y.: Public Affairs Press, 2011; Castells M. The Rise of the Network Society: The Information Age: Economy, Society, and Culture. John Wiley & Sons, 2011.

[54]Бачило И.Л. Информационное право. Учебник. / Бачило И.Л., Лопатин В.Н., Федотов М.А. СПб: «Юридический Центр», 2001; Бачило И. Л. Информационное право: Учебник для ВУЗов. М.: Высшее образование, Юрайт-Издат, 2009; Городов О. А. Информационное право. Учебник. М.: Проспект, 2009; Информационное право. Актуальные проблемы теории и практики /Под ред. Бачило И. Л. М.: Юрайт, 2008; Наумов В.Б. Право и Интернет: очерки теории и практики. М.: Книжный дом «Университет», 2002;Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт. М.: Норма, 2004; Серго А. Г. Интернет и право. М.: «Бестселлер», 2003.

[55] Kurbalija J. Internet governance and international law. URL: http://www.wgig.org/docs/book/Jovan_Kurbalija%20.pdf; Menthe D., Jurisdiction In Cyberspace: A Theory of International Spaces. // Michmann Telecommunication Technical Revue. № 69. URL: http://www.law.umich.edu/mttlr/vol-four/menthe.html; Schwabach A. Internet and the law: technology, society, and compromises. Santa Barbara: ABC-CLIO, 2005; Froomkin M. International and National Regulation of the Internet. // The Round Table Expert Group on Telecommunications Laws: Conference Papers / Ed. by Dommering E., Eijk N. Amsterdam, 2005. URL: http://law.tm/docs/International-regulation.pdf

[56] Lessig L. Code and other laws of cyberspace. N. Y.: Basic Books, 1999; Lessig L. The Future of Ideas. (The Fate of the Commons in a Connected World). – N. Y.: Random House, 2001.

[57] Tallinn Manual on the International Law Applicable to Cyber Warfare / ed. by M.Schmitt – N.Y.: Cambridge University Press, 2013.

Крутских, А.В. Коротков[58], а также зарубежных авторов С. Раушера, Л. Гринберга, С. Гудмана, К. Суху[59] и др.

Проблематика международного управления Интернетом в исследовательских работах и дипломатической риторике большинства государств сегодня связана с обеспечением информационной безопасности. От институциональной архитектуры управления на международном уровне зависят ключевые характеристики Интернета, и, следовательно, глобального информационного общества. Среди работ, посвященных международно-политическим аспектам управления Интернетом следует отметить монографию И. Курбалиа и Э. Гелбстайна, сборники статей под редакцией Д. Маклина и В. Кляйнвехтера, а также научные труды В. Даттона, Д. Дрезнера, Д. Маклина,М. Пелту, Д. Хоффман,[60]. Среди работ российских авторов можно назвать статьи Быкова А.И., Зиновьевой Е.С., Якушева М.В.[61] Кроме того, анализом процессов управления Интернетом с позиций теории международных режимов занимаются такие авторы как М. Франда, Д. Когбурн, М. Мюллер, Д. Матиасон и Х. Кляйн[62].

---

[58] Коротков А.В. Безопасность критических информационных инфраструктур в международном гуманитарном праве / А.В. Коротков, Е.С. Зиновьева // Вестник МГИМО-Университета. 2011. № 4. С. 154-162; Крутских А.В. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. 2007. № 1(5). С.28-37. URL:http://www.intertrends.ru/thirteen/003.htm;

[59] Rauscher K., Korotkov A. Working towards rules for governing cyber conflict. Rendering Geneva and Hague conventions in cyberspace // East-West institute. 2011. URL:http://www.ewi.info/working-towards-rules-governing-cyber-conflict; Greenberg L.T., Goodman S.E., Soo Hoo K.J. Information Warfare and International Law. Washington: National Defense University Press, 1997.

[60]Курбалийя Й., Гелбстайн Э. Управление Интернетом: проблемы, субъекты, преграды / Пер. с англ. Михеева А.Н., Лазуткиной А.В. М.: МГИМО, 2005; Internet Governance: A Grand Collaboration. / Ed. by MacLean D. N.Y.: UN ICT Task Force Series, 2005; The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment / Ed. By Kleinwächter W. Berlin: Wagner Translations Ltd., 2007; Drezner D. The Global Governance of the Internet: Bringing the State Back In. // Political Science Quarterly. 2004. № 3 (119). URL: http://www.danieldrezner.com/research/egovernance.pdf; Dutton W., M. Peltu. The emerging internet governance mosaic: connecting the pieces. // Discussion Paper No 5. // Oxford Internet Institute Forum. Oxford, 2005. URL: http://www.iospress.metapress.com/index/M14U6635863R0718.pdf; Hofmann J. Internet Governance: A Regulative Idea in Flux. // Social Science Research Centre. Berlin, 2005 URL: http://duplox.wzb.eu/people/jeanette/texte/Internet%20Governance%20english%20version.pdf; MacLean D. Herding cats: Some conceptual tools for thinking about Internet governance. // Internet Governance: a grand collaboration. An edited collection of papers. / Ed. by MacLean D. – N.Y.: UN ICT Task Force, 2004. P. 73-100.

[61] Быков А.И. Управление Интернетом как одна из проблем современных международных отношений. // Политэкс. URL: http://www.politex.info/content/view/438/30; Зиновьева Е. С. Российские интересы в сфере управления Интернетом //Международные процессы. 2009. №. 19. С. 101-108; Якушев М.В. Информационное общество и правовое регулирование: новые проблемы теории и практики // Информационное общество. 1999. № 1. URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/2be96a4e09339699c32568b1003ab653

[62] Franda M. Governing the Internet: The Emergence of an International Regime. — Boulder: Lynne Rienner Publishers, 2001; Franda M. Launching into cyberspace. Boulder: Lynne Rienner Publishers, 2002; Cogburn D. Globalization and Governance in Cyberspace: Mapping the Processes of Emergent Regime Formation in Global Information and Communications Policy. URL: http://arxiv.org/ftp/cs/papers/0109/0109052.pdf; Mueller M. The Internet and Global

Работы указанных авторов позволили сформировать комплексное представление о современных характеристиках режима управления Интернетом, интересах различных субъектов управления, а также перспективах интернационализации управления Интернетом. Кроме того, на основании анализа данной литературы удалось определить роль международного сотрудничества по управлению Интернетом в рамках складывающегося международного режима информационной безопасности, взаимное отношение этих двух предметных областей.

Анализу международной информационной безопасности посвящали свои труды такие авторы, как Аничкина Т.Б., Бедрицкий А.В., Гаджиев К.С., Крутских А.В., Панарин И.А., Роговский Е.А., Туронок С.Г, Федоров А.В., Черненко Е.В., Шариков П.А., Шерстюк В.П.[63]. Надо отметить, что официальная политическая и дипломатическая риторика по проблеме информационной безопасности РФ и стран Запада отличаются друг от друга, что,в свою очередь, повлияло на оценки исследователей и ученых. Для сопоставления конкурирующих академических дискурсов были использованы работы таких зарубежных авторов как А. Вегнер, В. Бенедек, Г. Джакомелло, М. Хансен, Х. Ниссенбаум, Г. Неунек, Г. Нохейм и др[64].Изучением проблем обеспечения национальной безопасности Российской

Governance: Principles and Norms for a New Regime. / Mueller M., Mathiason J., Klein H. // Global Governance. 2007. № 13. URL: http://www.atypon-link.com/LRP/doi/abs/10.5555/ggov.2007.13.2.237

[63] Аничкина Т.Б. О некоторых приемах информационной войны США. // США-Канада: экономика, политика, культура. 2007. №7. С. 123-127; Бедрицкий А.В. «Информационное доминирование» США и ассиметричное информационное противоборство. // США – Канада: экономика, политика, культура. 2007. №2; Крутских А.В., Федоров А.В. О международной информационной безопасности // Международная жизнь. 2000. №2. С. 37- 48; Роговский Е.А., Шариков П.А. Контроль над Интернетом и международная стабильность. // США – Канада: экономика, политика, культура. 2007. № 3. С. 93-111; Федоров А.В. Информационная безопасность в мировом политическом процессе. – М.: МГИМО, 2006; Роговский Е.А., Шариков П.А. Контроль над Интернетом и международная стабильность. // США – Канада: экономика, политика, культура. 2007. № 3; Роговский Е.А. Лидерство США в глобальных технология и международная безопасность // США – Канада: экономика, политика, культура. 2007. №9. С.53-70; Туронок С. Г. Информационно-коммуникативная революция и новый спектр военно-политических конфликтов // Политические исследования. 2003. № 1. С. 24-38; Роговский Е.А. Кибер-Вашингтон: глобальные амбиции. М.: Международные отношения, 2014; Черненко Е.В. Холодная война 2.0? Киберпространство как новая арена противостояния // Россия в глобальной политике. 2013. № 2. URL:http://www.globalaffairs.ru/number/Kholodnaya-voina-20-15874

[64] Benedek W. Internet Governance and the Information Society: Global Perspectives and European Dimensions. / Benedek W., Bauer V., Kettemann M. Utrecht: Eleven International Publishing, 2008. 176 p.; Wenger A. The Internet and the Changing Face of International Relations and Security // Information and Security. 2001. № 7. P. 5-11; Security in Cyberspace: Targeting Nations, Infrastructures, Individuals. / Ed by G. Giacomello – Bloomsbury Publishing USA, 2014; Hansen L., Nissenbaum H. Digital disaster, cyber security, and the Copenhagen School //International Studies Quarterly. 2009. №. 4. P. 1155-1175; Neuneck G. Civilian and military cyberthreats: shifting identities an attribution. // The Cyber Index. International Security Trends and Realities. UNIDIR, 2013. URL:

Федерации в цифровую эпоху занимаются Швец Д.Ю., Смирнов А.И., Кучерявый М.М. и др.[65]

Для того чтобы оценить особенности объекта безопасности, потребовалось ознакомиться с работами, посвященными влиянию Интернета и других ИКТ на общество и политические процессы. Подобная тематика приобретает в последние годы все большую популярность как в России, так и за рубежом. Среди российских авторов, занимающихся разработкой данной проблематики, следует назвать Вершинина М.С., Пескова Д.Н., Роговского Е.А., Соловьева А.И., и др[66]. Такие зарубежные исследователи, как А. Шапиро, А. Чадвиг и П. Ховард[67], также занимаются исследованиями этих вопросов.

Вопросы обеспечения безопасности критических информационных инфраструктур исследуют Коротков А.В., Кононов А.А., Черешкин Д.С., Васенин Д.А.[68] и др. Среди зарубежных изданий в этой области наиболее авторитетным является ежегодная Хрестоматия по вопросам защиты критических инфраструктур, редакторами которой выступают А. Вегнер, В. Мауэр, М. Кавелти[69].

---

http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf; Nojeim G. Statement On Cybersecurity, Civil Liberties and Innovation. // US Senate House Committee on Energy and Commerce, Subcommittee on Communications, Technology and the Internet. – Washington D.C., 1st may 2009. URL:http://www.cdt.org/security/20090501_cybersecurity.pdf

[65] Швец Д.Ю. Информационная безопасность Российской Федерации в современных международных отношениях. Дисс. … кандидата социологических наук. М.: МГИМО (У) МИД России, 2005; Глобальная безопасность: инновационные методы анализа конфликтов / под ред. А.И. Смирнова– М: Общество «Знание» России, 2011; Кучерявый, М. М. Глобальное информационное общество и проблемы безопасности // Власть. Общенациональный научно-политический журнал. 2013. № 9 (сентябрь). С. 89-92; Кучерявый, М. М. Основные направления государственной политики РФ в области обеспечения международной информационной безопасности // Власть. Общенациональный научно-политический журнал. 2013. № 12 (декабрь). С. 54-59.

[66] Вершинин М.С. Политическая коммуникация в информационном обществе СПб.: Изд-во Михайлова В.А., 2001; Песков Д.Н. Интернет в российской политике: утопия и реальность. // Полис. 2002. № 1. С. 31-45;Песков Д.Н. Интернет в России: политическая утопия? URL: http://www.nethistory.ru/biblio/1040595057.html; Роговский Е.А. США информационное общество: экономика и политика. М.: Международные отношения, 2008; Политические коммуникации. Учебное пособие. / под. ред. Соловьева А.И. М.: Аспект Пресс, 2004.

[67] Chadwick A., Howard P. Routledge Handbook of Internet Politics. London: Taylor & Francis, 2008; Shapiro A. The control revolution: how the Internet is putting individuals in charge and changing the world we know. N.Y.: Public Affairs, 1999.

[68] Коротков А.В. Безопасность критических информационных инфраструктур в международном гуманитарном праве / А.В. Коротков, Е.С. Зиновьева // Вестник МГИМО-Университета. 2011. № 4. С. 154-162; Кононов А.А., Черешкин Д.С. Ключевые проблемы обеспечения безопасности национальной информационной инфраструктуры // Информационное общество. 2002. № 1. С 8-18; Критически важные объекты и кибертерроризм. Ч.1. / Под ред. В.А. Васенина. М.: МЦНМО, 2008.

[69] International critical information infrastructure protection handbook 2008 / 2009 / Ed. by A. Wenger, V. Mauer, M. Cavelty. ETH Zurich: Center for Security Studies, 2009.

Многие зарубежные политологи исследуют вопросы информационного противоборства. Среди наиболее известных трудов можно отметить работы М. Либики, Р. Моландера, А. Шафрански, Р. Кларка и др.[70] Российские авторы также занимаются этой проблематикой, в их числе Р.В. Болгов, С.Г. Туронок, А.В. Манойло, Бедрицкий А.В. [71]

Большая часть работ российских авторов, занимающихся анализом международной информационной безопасности с позиций науки о международных отношениях или политологии, посвящена военно-политическим аспектам проблематики, вместе с тем, вопросы кибер-терроризма и кибер-преступности остаются малоизученными. В ходе анализа этих вопросов в настоящей работе были использованы в основном труды западных исследователей, таких как Л. Джанчевский, А. Коларик, И. Лачоу, К. Вилсон, С. Бреннер[72] и др. Однако и в западной литературе эти проблемы рассматриваются не столь пристально, как военно-политические аспекты проблематики.

В течение последних лет в России был защищен целый ряд диссертаций, посвященных исследованию информационной безопасности и информационного противоборства с политологической точки зрения. Военным аспектам использования ИКТ и их роли в военных стратегиях западных стран посвящена диссертация на соискание ученой степени кандидата политических наук Болгова Р.В[73]. Батуева Е.В. в диссертации на соискание ученой степени кандидата политических наук исследует концепцию угроз кибербезопасности США и ее

---

[70]Libicki M. Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND Corporation, 2009; Molander R. Strategic Information Warfare: A New Face of War / R. Molander, A. Riddile, P. Wilson. CA: Rand Corporation, 1996; Szafranski R. A Theory of Information Warfare: Preparing for 2020 // Airpower Journal, 1995 №1; Clarke R. A., Knake R. K. Cyber war. TantorMedia, Incorporated, 2014.

[71] Болгов Р.В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях // Дисс. … ученой степени кандидата политических наук. СПб: СПбГУ, 2011; Бедрицкий А.В. «Информационное доминирование» США и асимметричное информационное противоборство // США – Канада: экономика, политика, культура. 2007. № 2; Туронок С.Г. Информационно-коммуникативная революция и новый спектр военно-политических конфликтов // Политические исследования. 2003. № 1. С. 24-38; Манойло А.В. Объекты и субъекты информационного противоборства // Пси фактор, 2003. URL: http://psyfactor.org/lib/psywar24.htm

[72] Zacher M., Sutton B. Governing Global Networks: International Regimes for Transportation and Communication. NY: Cambridge University Press, 1996; Curtis T. The International Telecommunication Regimes in the Information Age // Prometheus. 2003. No 4 (21). P. 399-414; Drake W. The Rise and Decline of the International Telecommunication Regime // Regulating global information society / Ed. by Ch. Masrsden – London: Routledge, 2000. P. 124-178; Siochru S. Global Media Governance: A Beginner s Guide. / Siochru S., Girard B., Mahan A. Lanham: Rowman & Littlefield, 2002.

[73] Болгов Р.В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях // Дисс. … ученой степени кандидата политических наук. СПб: СПбГУ, 2011.

влияние на международную безопасность[74]. Схожей теме посвящены диссертации Шарикова П.А. анализирующая политику США в области информационной безопасности[75] и Карасева П.А., исследующего политику безопасности США в глобальном информационном пространстве[76]. Докторская диссертация профессора МГУ Манойло А.В. была посвящена роли культурно-цивилизационных моделей и технологий информационно-психологического воздействия в разрешении международных конфликтов, и ориентирована на расширительное толкование информационной безопасности[77].Докторская диссертация Кучерявого М.М. посвящена трансформации категории национальной безопасностив информационную эпоху[78]. Однако, проблематика международного сотрудничества в сфере информационной безопасности в российской политологической науке пока не нашла комплексного отражения.

Как представляется, рассмотренные выше пласты литературы мало информированы друг о друге и мало цитируют друг друга. Исследователи, работающие в области теории международных отношений, в особенности занимающиеся проблемами международного сотрудничества, уделяют мало внимания исследованию вызовов цифровой среды. Более того, специальная литература в области информационной безопасности, информационного противоборства, кибер-терроризма и киберпреступности в основном ориентирована на лиц, принимающих решения, и не занимается исследованием международного сотрудничества в данной области с позиций теории международных отношений.

---

[74] Батуева Е.В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая // Дисс. … ученой степени кандидата политических наук. М.: МГИМО, 2015.

[75] Шариков П.А. Политика США в области информационной безопасности // Дисс. … ученой степени кандидата политических наук. М.: ИСКРАН, 2009.

[76] Карасев П.А. Политика безопасности США в глобальном информационном пространстве. Автореферат дис. на соискание … к.полит.н. М.: ИМЭМО РАН, 2015. URL: https://www.imemo.ru/files/File/ru/dis/2015_004_Karasiov_AUTR.pdf

[77] Манойло А.В. Роль культурно-цивилизационных моделей и технологий информационно-психологического воздействия в разрешении международных конфликтов // Дисс. … ученой степени доктора политических наук. М.: МГУ, 2010.

[78]Кучерявый М.М. Информационное измерение политики национальной безопасности России в условиях современного глобального мира // Дисс. … ученой степени доктора политических наук. СПб: СПбГУ, 2014.

Анализ официальных источников и научной литературы по проблемам обеспечения международной информационной безопасности показал, что транснациональный характер информационных вызовов и угроз обуславливает необходимость международного сотрудничества с привлечением государств, бизнеса и гражданского общества. Однако проблемы поиска оптимального институционального дизайна и выявления перспективных направлениях сотрудничества в теоретическом плане подробно не освещаются ни в российской, ни в зарубежной научной литературе.

Источниковая база исследования включает две группы источников. В первую группу вошли официальные документы государств, прежде всего, России, США, Китая, которые позволили сформировать представление о национальных интересах и государственной политике государств в отношении информационной и кибер безопасности, а также о внешнеполитической стратегии в рассматриваемой области международных отношений.

Вторую группу источников составили официальные документы международных организаций и форумов, задействованных в формировании международных режимов по обеспечению информационной безопасности на глобальном и региональном уровнях. Среди международных организаций глобального уровня, следует отметить ООН, как организацию, обладающую наибольшей легитимностью и универсальным представительством, что обуславливает ее особую роль в формирующемся глобальном режиме международной информационной безопасности. Такие специализированные организации «семьи ООН», как МСЭ и МАГАТЭ, регулируют вопросы технологических аспектов глобальной информационной безопасности и международной безопасности компьютерных систем, обеспечивающих работу мирного атома (последняя сфера привлекает все большее внимание в последние годы). Кроме того, усиливается влияние организаций т.н. «клубного типа», таких как Группа семи, БРИКС, в том числе и в обеспечении информационной безопасности. Среди региональных структур особое внимание было уделено

организациям, в работе которых принимает Россия – СНГ, ОДКБ, ШОС, Совет Европы. В работе также был изучен опыт региональных структур, в рамках которых развивается взаимодействие в исследуемой области, прежде всего, ЕС, НАТО, а также АСЕАН. Изучение документов выше обозначенных организаций позволило получить представление об основных направлениях деятельности данных организаций, о характере международных переговоров в исследуемой области, о ходе имплементации достигнутых соглашений.

Кроме того, были использованы документы, заложившие основу международного гуманитарного права, а также отдельные документы неправительственных организаций, занимающихся вопросами международного управления Интернетом, таких как ICANN.

Научная новизна работы заключается в следующем**:**

- доказательстве того, что логика международного сотрудничества в сфере обеспечения информационной безопасности соответствует единой логике сотрудничества в международных отношениях. Несмотря на то, что предмет сотрудничества является относительно новым и специфичным для международных отношений, логика взаимодействия государств, участвующих в переговорах поданной проблематики, мало чем отличается от логики взаимодействия в других сферах международных отношений. Данный вывод является нетривиальным, поскольку информационное пространство и в частности Интернет, как правило, рассматривается в качестве абсолютно новой сферы международных отношений, в рамках которой логика международного взаимодействия будет отличаться от логики взаимодействия в других сферах. С позиций теории кейс-стади, кейс информационной безопасности представляет собой отклоняющийся кейс, исследование которого представляет особую значимость с теоретической точки зрения. Таким образом, проведенное исследование вносит вклад, с одной стороны, в исследования теории международных отношений, а именно ее направления, связанного с

концептуализацией развития науки и технологий, в том числе ИКТ и информационной безопасности, а также вносит вклад в развитие теории информационного общества. Более того, подобная логика подтверждается на основании анализа трех кейсов международного взаимодействия (в области контроля над ядерными вооружениями, освоения околоземного космического пространства и информационной безопасности и управления интернетом).

- впервые в российской литературе был проведен комплексный анализ складывающегося режима информационной безопасности, в том числе и с позиций значимых интересов России в данной области. Анализ был проведен на базе основных теоретических наработок в исследуемой области и с учетом актуальных практических реалий в России и в мире.

- установлено, что формирующийся глобальный режим информационной безопасности пока существует в форме активных переговоров и согласований позиций между ключевыми участниками информационной безопасности. Всеми разделяемые принципы, правила, нормы и процедуры принятия решений в данном режиме, по которым у ведущих игроков происходит совпадение ожиданий, пока не сформировались. Это объясняется высокой значимостью обсуждаемых вопросов.

- было исследовано не только глобальное, но и региональное измерение международного сотрудничества в сфере обеспечения информационной безопасности. Формирующийся режим информационной безопасности имеет специфику в различных международно-политических регионах.

- установлено, что формирующийся режим информационной безопасности находится в точке бифуркации, после которой он может пойти либо по укреплению глобального уровня сотрудничества, либо по развитию регионального уровня в ущерб глобальному.

- показано, что существующие тенденции международного сотрудничества свидетельствуют о развитии режима информационной безопасности с высокой

вероятностью в региональном направлении, что отражает общие тектонические сдвиги в системе международных отношений, направленные на укрепление многополярности в международных отношениях. Глобальный режим информационной безопасности, скорее всего тоже будет многополярным с ярко выраженной региональной динамикой.

- доказано, что развитие международного режима в направлении регионализации соответствует национальным интересам России.

- были определены направления развития международного сотрудничества в сфере информационной безопасности, сформулированы предложения по развитию международного регулирования.

- была концептуализирована роль социальных медиа во внешней политике и обеспечении информационной безопасности государств, а также в обеспечении международной информационной безопасности, что имеет как теоретическое, так и прикладное значение, так как данная проблематика является одной из активно обсуждаемых на международной повестке дня.

- был проведен анализ международного режима управления Интернетом с позиций значимых интересов РФ, предложена эффективная и отвечающая интересам нашей страны стратегия участия России в процессах формирования глобального режима управления Интернетом (в первую очередь с точки зрения использования потенциала международных организаций и институтов).

Теоретическая и практическая значимость работы заключается в том, что полученные выводы:

- вносят вклад в концептуализацию научно-технологического измерения современной мировой политики в теории международных отношений на основании анализа такой области, как развитие глобального информационного пространства;

- позволяют получить целостное представление о последствиях развития Интернета и формирования глобального информационного пространства для мировой системы, в том числе в контексте ее безопасного развития – таким образом, вносят вклад в развитие теории информационного общества;

- вносят роль в концептуализацию роли негосударственных акторов в современной мировой политике с позиций их участия в международных режимах на глобальном, региональном и транснациональном уровнях;

- позволяют получить комплексное представление о современных вызовах и угрозах международной информационной и кибер-безопасности, субъектах безопасности, различных теоретических подходах к изучению данной проблематики и их влиянии на внешнеполитическую деятельность государств и природу международного сотрудничества в исследуемой области;

- представляют собой комплексное изучение международного сотрудничества по обеспечению информационной безопасности, проведенное на основе методологии теории международных отношений, что дает возможность сформулировать перспективные тенденции развития исследуемой области;

- могут быть использованы с целью повышения эффективности деятельности органов государственной власти по продвижению интересов РФ в сфере международного сотрудничества по обеспечению информационной безопасности и управления Интернетом. В результате исследования, автор пришел к выводу, что регионализация международного взаимодействия по вопросам информационной безопасности создает условия для развития взаимодействия в рамках ШОС по вопросам обеспечения безопасности от «триады» угроз информационной безопасности (преступной, террористической и военно-политической), а также по противодействию «цветным революциям», инспирируемым по информационным каналам. Кроме того, сформулированы рекомендации по продвижению интересов России на глобальном уровне, в рамках таких организаций, как ООН и МСЭ. В частности, после появления инструментов,

позволяющих эффективно обрабатывать «большие данные» о пользователях социальных сетей и использовать их в политических целях, Россия заинтересована в развитии международного взаимодействия по вопросам защиты прав человека в цифровую эпоху.

Положения, выносимые на защиту:

1. Формирование международного режима информационной безопасности на глобальном уровне находится в стадии определения повестки дня. Взаимодействие между ведущими участниками мировой политики на этом уровне по данному вопросу протекает в режиме торга. При этом торг носит скорее «маскировочный» характер, так как стороны выдвигают заведомо неприемлемые друг для друга предложения, занимаясь параллельно наращиванием военного потенциала в сфере информационного безопасности. Реальные интересы и позиции сторон в значительной степени засекречены и непрозрачны. Информационная безопасность как сфера межгосударственного взаимодействия на глобальном уровне, таким образом, секьюритизирована. Сотрудничество наблюдается по неполитизированным или частично политизированным вопросам, таким как техническая координация Интернета, взаимодействие между специальными группами по противодействию киберпреступности и реагированию на киберинцеденты (Центрами по предотвращению компьютерных инцидентов, CERT), техническая координация и стандартизация.
2. Современный этап развития информационного общества характеризуется регионализацией, что находит свое отражение в динамике трансграничных потоков информации. В этих условиях формирование региональных режимов информационной безопасности определяется спецификой отношений между государствами внутри региона, а также восприятием приоритетности и характера вызовов и угроз информационной безопасности / кибербезопасности государствами региона. В отдельных регионах сформировались режимы информационной безопасности, была выработана повестка дня, достигнуты договоренности по согласованным вопросам и начата имплементация

достигнутых решений: К числу таких регионов можно отнести Евроатлантический регион в рамках НАТО, Юго-восточная Азия в рамках АСЕАН, постсоветские государства в рамках ОДКБ[79].

3. Двусторонние соглашения заключаются, с одной стороны, между государствами, обладающими значительными кибер-потенциалами (и воспринимающими друг друга как угрозу) и направлены на формирование мер доверия и предотвращение инцидентов, а с другой – между влиятельными в информационной сфере государствами и их союзниками (государствами, разделяющими общее видение угроз информационной или кибер-безопасности), что позволяет усилить переговорные позиции на глобальных площадках. К их числу соглашений первого типа можно отнести двусторонние договоренности между такими странами, как Россия и США, США и Китай, Россия и Китай. Таким образом, на сегодняшний день сложилась сетка двусторонних договоренностей в области информационной безопасности, дополняющая региональное взаимодействие в данной области.
4. Формирование режима информационной безопасности на глобальном уровне повторяет в своем развитии логику формирования режима ядерного нераспространения и режима космической безопасности. Переход от стадии определения повестки дня к переговорному процессу и впоследствии имплементации достигнутых соглашений в данных областях был возможен лишь в условиях осознания государствами общей уязвимости в результате возможного военного использования новых технологий. Ключевой предпосылкой складывания эффективного режима информационной безопасности на глобальном уровне является осознание участниками режима баланса угроз. Осознание баланса угроз возникает в ходе острых международных кризисов, таких как Карибский кризис в случае с ракетно-ядерным оружием, или при демонстрации разрушительной силы накопленных потенциалов, как при испытании ядерного оружия или бомбардировках Хиросимы и Нагасаки. В сфере

[79]В российской науке о международных отношениях был предложен новый термин «Центральная Евразия» для обозначения современной региональной динамики (см. К великому океану – 3. Создание Центральной Евразии // Аналитический доклад Международного Дискуссионного клуба «Валдай». М., 2015. URL: http://iwep.kz/files/attachments/article/2015-04-21/doklad_sozdanie_evrazii_ekonomicheskiy_poyas_shelkovogo_puti.pdf

информационной безопасности, невзирая на разоблачения Э. Сноудена столь кризиса пока не произошло, причем ситуация осложняется спецификой информационного оружия – сложностью идентификации источника атаки, доступностью и эффективностью наступательных вооружений в информационном пространстве, а также асимметрией наступательных и оборонительных вооружений (в настоящее время наступательное информационное оружие гораздо эффективнее оборонительного).

5. На современном этапе развития США стремятся упрочить лидерство в сфере управления Интернетом и информационной безопасности. В этих условиях США не заинтересованы в развитии и институционализации международного сотрудничества на глобальном уровне по обеспечению информационной безопасности, желая сохранить «свободу рук» в развитии и военном применении ИКТ, в том числе информационного оружия (за исключением выработки правил применения норм международного гуманитарного права к информационной сфере, что позволит легитимировать использование информационного оружия на государственном уровне, подчинив его международно-правовой регламентации). Однако, постепенное распространение новых технологий подрывает лидерство США, что вероятность интенсификации международного сотрудничества по обеспечению информационной безопасности США, однако на двустороннем и региональном, а не глобальном уровне.
6. В условиях глобальной информатизации происходит диффузия власти, усиливаются позиции негосударственных акторов мировой политики – бизнес-структур, МНПО, представителей исследовательского сообщества. Крупные бизнес-структуры имеют возможность влиять на позиции государств, ход международных переговоров, а также участвуют в имплементации достигнутых соглашений. Более того, региональные бизнес-структуры (за исключением компаний, базирующихся в США) поддерживают регионализацию режимов информационной безопасности, так как такие режимы защищают их от конкуренции со стороны глобальных игроков. МНПО и представители исследовательского сообщества обладают значительным влиянием в рамках

технических режимов управления Интернетом и обеспечения информационной безопасности, в частности, они вырабатывают стандарты использования Интернета и обеспечения информационной безопасности. В этих условиях формируются новые модели международного сотрудничества государств и негосударственных акторов, многосторонние партнерства (также используется термин многоуровневое сотрудничество). Роль многосторонних партнёрств в сфере информационной безопасности будет возрастать, однако, при координирующей роли государств. Таким образом, государства являются ключевыми, но не единственными субъектами формирующегося режима международной информационной безопасности, негосударственные акторы выступают в роли секьюритизирующих субъектов (имеют возможность влиять на процессы выработки государствами дискурса информационной безопасности), а также участвуют в имплементации уже согласованных на межгосударственном уровне региональных режимов информационной безопасности и глобального режима управления интернетом.

7. Усиливается тенденция к секьюритизации международного управления Интернетом, что является составной частью более широкой проблемы обеспечения международной информационной безопасности. Передача в 2016 г. функций управления пространством имен и адресов интернета, критической технологической инфраструктурой, обеспечивающей функционирование интернета на глобальном уровне, от Internet Corporation for Assigned Names and Numbers (ICANN), частной некоммерческой организации, имеющей контрактные отношения с правительством США, к ее дочерней организации Public Technical Identifiers (PTI)[80], которая напрямую не связана с правительством США, не решила проблемы с подотчетностью и международной легитимностью сложившейся системы управления интернетом. Государства, ключевые субъекты формирующегося глобального режима международной информационной безопасности, не имеют возможности влиять на принимаемые организацией

[80]IANA Naming Function Contract. 30 September 2016. URL: https://www.icann.org/iana_pti_docs/151-iana-naming-function-contract-v-30sep16

решения. В настоящее время на международном уровне ведутся переговоры об интернационализации управления Интернетом (полной или частичной передачи функции администрирования пространства имен и адресов интернета на уровень межправительственной организации), существующую модель управления оспаривают все большее количество государств. Обсуждается создание альтернативных (региональных) проектов Интернета в случае сохранения существующей модели управления, что может подорвать потенциал сети и не соответствует интересам ведущих игроков. Таким образом, реформа управления адресным пространством глобальной сети не снимает существующих межгосударственных противоречий по вопросу управления интернетом.

8. Россия заинтересована регионализации режима информационной безопасности. России удалось сформировать режим информационной безопасности на постсоветском пространстве на основе ОДКБ, формирование международного сотрудничества в рамках ШОС на более широком евразийском пространстве находится на этапе согласования позиций. Взаимодействие по вопросам информационной безопасности на постсоветском пространстве ставит своей задачей обеспечение информационной безопасности стран-членов организации (противодействие триде угроз информационной безопасности – преступной, террористической и военно-политической), а также направлено на противодействие «цветным революциям», инспирируемых по информационным каналам (в том числе с использованием социальных сетей и новых медиа).
9. Наиболее дискуссионным объектом информационной безопасности является гражданское общество в информационной стадии своего развития. Если общество вошло в информационную стадию своего развития, то обеспечение информационной безопасности для такого общества является противоречием в понятиях. Гражданское общество на такой стадии развития представляет собой открытую систему, взаимодействующую с глобальной информационной средой, что делает его более устойчивым по сравнению с закрытыми системам. Информационное общество умеет работать с информацией и, следовательно, имеет иммунитет против внешнего информационного манипулирования. Вместе с

тем, формирование информационного общества предполагает увеличение зависимости всех сфер жизни общества и государства от информационной инфраструктуры, вследствие чего уязвимыми становятся критические информационные инфраструктуры. Обеспечение безопасности критических информационных инфраструктур в силу транснационального характера вызовов и угроз невозможно без международного взаимодействия на уровне государств; таким образом, обеспечение информационной безопасности предполагает сотрудничество сильного гражданского общества и сильного государства.

Основные результаты исследования прошли апробацию на международных и российских научных конференциях. Результаты исследования также отражены в учебных публикациях автора, 1 авторском учебном пособии, а также в 7 разделах в учебниках и учебных пособиях, 2 авторских монографиях по теме диссертационного исследования, а также 2 разделах в коллективных монографиях, 3 статьях в научных изданиях, входящих в базу данных **Scopus**, а также в следующих статьях в научных журналах из списка **ВАК**:

1. Зиновьева Е.С. Интернационализация управления Интернетом — США сдают позиции? // США и Канада: экономика, политика, культура. - 2009. №8.
2. Зиновьева Е.С. Российские интересы в сфере управления Интернетом // Международные процессы. 2009. № 1 (19).
3. Зиновьева Е.С. Международное управление Интернетом: проблемы, подходы, перспективы // Вестник МГИМО-Университета. 2010. № 6.
4. Коротков А.В., Зиновьева Е.С. Безопасность критических информационных инфраструктур в международном гуманитарном праве // Вестник МГИМО-Университета. 2011. № 4.
5. Зиновьева Е.С. Развитие информационного общества: проблемы безопасности // Вестник МГИМО-Университета. 2012. № 1.
6. Зиновьева Е.С. Размышления на тему кризиса // Вестник МГИМО-Университета. 2012. № 1.

7. Зиновьева Е.С. Цифровая дипломатия США: возможности и угрозы для международной безопасности // Индекс Безопасности. 2013. № 1(104).
8. Зиновьева Е.С. Международно-политические аспекты развития сети Интернет // Вестник МГИМО-Университета. 2013. № 4.
9. Зиновьева Е.С. Воздействие компаний Интернет-индустрии на мировую политику // Вестник МГИМО-Университета. 2013. № 1.
10. Зиновьева Е.С., Фатуева Е.В. Развитие мировой политической системы и глобальное управление // Вестник СПбГУ. Серия 6: философия, культурология, политология, право, международные отношения. - 2014. №4.
11. Зиновьева Е.С. Анализ внешнеполитических инициатив России в области международной информационной безопасности // Вестник МГИМО-Университета. 2014. № 6.
12. Крутских А.В., Зиновьева Е.С. Информатизация и макротехнологии. Новое лицо мировой политики // Международные процессы. 2014. № 36-37.
13. Зиновьева Е. Международное сотрудничество по обеспечению информационной безопасности // Право и управление. XXI век. - 2014. - № 4.
14. Болгов Р.В., Зиновьева Е.С., Карачай В.А. Развитие информационного общества в странах Таможенного Союза: правовые аспекты // Управленческое консультирование. 2015. № 1.
15. Зиновьева Е.С., Казанцев А.А. Сложность мировой политики: к вопросу о новой методологии анализа // Мировая экономика и международные отношения, 2015. № 4.
16. Зиновьева Е.С. Инновационное развитие мира // Сравнительная политика. 2015. № 4.
17. Зиновьева Е.С. Глобальное управление Интернетом в контексте международной безопасности // Вестник МГИМО-Университета. 2015. № 4.
18. Зиновьева Е.С. Роль социальных медиа в современных международных конфликтах: существующие научные подходы и перспективные направления исследований // Национальная безопасность / nota bene. — 2016. № 3. С.358-368.

19. Зиновьева Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности // МГИМО-Университета. 2016. № 4.
20. Лебедева М.М., Харкевич М.В., Зиновьева Е.С., Копосова Е.Н. Архаизация государства: роль современных информационных технологий // Полис. 2016. № 6. С. 22-36.

21.

ГЛАВА 1. ВЛИЯНИЕ ИНФОРМАЦИОННОЙ РЕВОЛЮЦИИ НА МИРОВУЮ ПОЛИТИКУ

1.1. Научно-технологическое измерение мировой политики: теоретико-методологические основания анализа

1.1.1. Мирополитическая концептуализация научно-технологического развития

Исследование научно-технологической составляющей мировой политики предоставляет исторические аналогии и теоретико-методологическую базу, необходимую для понимания взаимных связей между технологическими трансформациями и международной политикой, в том числе и современной информационной революцией и международной безопасностью (такими авторитетными авторами, как Э. Тоффлер, Д. Белл и др., информационная революция трактуется как технологическая трансформация, связанная с появлением новых способов передачи и хранения информации, повлекшая за собой революционные изменения во всех сферах жизни общества и государства)[81]. Таким образом, подобный подход позволит оценить влияние современной информационной революции на международную безопасность.

[81]Термин «информационная революция» связан с теоретической концепцией информационного общества, разрабатываемой такими авторами, как Д. Белл, Э. Тоффлер и др. С точки зрения вышеперечисленных авторов информационных революций в истории человечества было несколько и связаны они были с возникновением новых инструментальных способов передачи и хранения информации — письменности, печатного станка, компьютера, что впоследствии способствовало революционным изменениям во всех сферах жизни общества и государства. Современная информационная революция датируется началом 1990-х гг. и связана с широким распространением пользовательских компьютеров и сети Интернет. Как правило, современная информационная революция трактуется как связанная с развитием информационно-коммуникационных технологий, а именно, компьютерных и телекоммуникационных технологий, а также постоянной динамической интеграцией этих технологий в единую глобальную мультимедийную систему. Несмотря на существующие различия в подходах к определению сущности и последствий информационной революции, большая часть исследователей соглашается ее трактовкой как революционных информационно-технологических изменений, повлекших за собой трансформации во всех сферах жизни общества и государства. (Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования / Перевод с английского. Изд. 2-ое, испр. и доп. - М.: Academia, 2004; Тоффлер Э. Третья волна. - М.: ООО «Издательство АСТ», 1999 и др.).

Научно-технологическая сфера и политика развиваются синхронно, оказывая взаимное влияние друг на друга. В различные периоды мировой истории интенсивность взаимного влияния варьировалась. Теория международных отношений уделяет относительно мало вниманию изучению специфики взаимного влияния мировой политики и технологий, в отличие отряда других гуманитарных дисциплин, в частности философии, где сформировалось отдельное направление, посвященное анализу роли науки и технологий в соответствующей предметной области – а именно, философия технологий. Значительная часть исследований в области мировой политики лишь косвенно затрагивает вопросы технологического развития, однако подспудно находится под влиянием парадигмы технологического детерминизма (в качестве примера можно привести работы авторов, исследующих процессы информатизации и влияние информационной революции на общественное развитие и, в том числе, мировую политику, в частности, Д. Белла[82], А. Тоффлера[83], а также российских авторов, Балуева Д.Г.[84], Кашлева Ю.Б.[85], Пескова Д.Н.[86] и др., которые рассматривали информационную революцию как движущую силу общественных трансформаций, в частности, перехода от индустриального общества к постиндустриальному, а в области международной политики развитие информационно-коммуникационных технологий – как ключевой драйвер глобализации, размывания государственного суверенитета, выхода новых акторов на международную арену). В рамках технологического детерминизма технологии рассматриваются как независимый, фактически автономный агент общественных изменений. Его популярность обусловлена тем, что технологические факторы носят явный характер, создавая иллюзию прочной причинно-следственной связи. Критики технологического детерминизма ставят вопрос о возможности

[82] Белл Д. Грядущее постиндустриальное общество: опыт социального прогнозирования: пер. с англ. М.: Academia, 1999. 788 с.
[83] Toffler A. Powershift: Knowledge, Wealth, and Violence in the 21st Century. N.Y.: BantamBooks, 1990 640 p.
[84] Балуев Д.Г. Информационная революция и современные международные отношения Нижний Новгород, 2001. 108 с.
[85] Кашлев Ю.Б. Информационный взрыв: международный аспект. М.: Международные отношения, 1988. 208 с.
[86] Песков Д.Н. Интернет в мировой политике: формы и вызовы // Современные международные отношения и мировая политика / Отв. ред. А.В. Торкунов; МГИМО(У) МИД России. М.: Просвещение, 2004. С. 155-172.

приписывать субъектность (роль агента) технологии, ведь технологии – это, прежде всего, продукт деятельности людей. Таким образом, согласно критикам данного подхода история технологий – это продукт человеческой деятельности, вписанная в сложный социальный, экономический, политический и культурный контекст[87]. Настоящее исследование также исходит из ограниченности детерминистического подхода и ориентировано на признании значимости взаимного влияния характеристик международной политики и технологий.

В целом, исследователи-международники мало занимаются изучением взаимного влияния научно-технического развития и мировой политики. При этом, как уже было отмечено, большая часть исследований посвящена влиянию науки и технологий на международную политику и носит детерминистический характер. Так, «американский исследователь, профессор Массачусетского технологического института Е. Скольников резюмировал основные каналы влияния науки и технологий на мировую политику[88]:

– изменение баланса сил, международного порядка, его структуры, принципов организации, взаимоотношений между субъектами международной политики (научно-технический потенциал во многом определяет уровень экономического развития государства, а стало быть, его военную мощь и – в целом – потенциал влияния на международной арене);

– трансформация процессов, протекающих в международной системе, а именно: дипломатии и переговоров, войны и конфликтов, международной торговли и иных экономических взаимоотношений (например, разработка систем космической навигации и высокоточного оружия стали основой современной «революции в военном деле»);

– появление новых возможностей и ограничений во внешней политике государств, не только политических, но и социальных, позволяющих обойти

[87] Does technology drive history. The dilemma of technological determinism. / Ed by M. Smith, L. Marx MIT Press, 1994. 298 p.
[88] Skolnikoff E. B. The elusive transformation: science, technology, and the evolution of international politics. Princeton University Press, 1994.P. 7.

физические, природные барьеры (например, возможность проецировать военную силу в различные точки планеты);

– создание новых образов, на основании которых мы воспринимаем международную действительность, теоретических концепций мировой политики и информационных ресурсов для принятия внешнеполитических решений (как отмечает в этой связи российский политолог М.М. Лебедева, если в годы «холодной войны» осмысление глобальной политики происходило в терминах ядерной физики «ядра» и «периферии», то в настоящее время мир мыслится как сложная сеть наподобие Интернета[89])»[90].

Подход Е. Скольникова может быть дополнен концептуализацией обратного влияния – мировой политики на науку и технологии. Как отмечает Д. Херрера, любая технология тесно связана с политикой, так как, во-первых, определение ключевых характеристик технологий является предметом политических противоречий, а во-вторых, любая технология предполагает формирование практических знаний, воплощенных в материальных результатах ее использования, а также институтах, необходимых для управления ее развитием и использованием[91].При этом, если на начальном этапе развития инновационных технологий их свойства, определяемые экспертным сообществом, участвующим в разработке технологий и последующей координации их использования, в значительной степени способны влиять на общественные отношения, в том числе и в сфере международной политики, то на более поздних этапах характеристики политики, в том числе международной, в значительной степени определяют направления эволюции и использования технологий.

Говоря о взаимном влиянии науки и технологий и мировую политики, необходимо вкратце охарактеризовать актуальные тенденции технологического развития, в том числе в сфере информационных технологий.

---

[89] Лебедева М.М. Мировая политика. М.: Аспект-Пресс, 2007. С. 243.

[90]Крутских А.В., Зиновьева Е.С. Информатизация и макротехнологии. Новое лицо мировой политики. // Международные процессы. 2014. №. 36-37. С. 20.

[91]Herrera G. L. Technology and international systems //Millennium-Journal of International Studies. 2003. №. 3. P. 559.

С одной стороны, возрастает скорость научно-технических изменений, а с другой – степень их проникновения в различные сферы жизни общества и государства. Роль и место государства международной арене в значительной мере определяются уровнем развития технологий, науки и образования. Научно-технологический процесс способствует процессам глобализации и усиления взаимозависимости, ускоряет формирование многополярного мира, так как технологии по своей сути транснациональный и быстро распространяются по миру. Однако сохраняющаяся асимметрия доступа к научным достижениям способствует закреплению неравенства в мире, порождает соперничество за обладание передовыми технологиями, обостряет существующие международные противоречия. Примером может послужить т.н. «цифровой разрыв» - неравномерное развитие информационных технологий между странами, регионами, внутри государств.

Государства сохраняют свое влияние как ключевых акторов научно-технологической сферы, но вынуждены считаться с новыми участниками международного взаимодействия в данной области, в частности, с бизнес-структурами. Бизнес становится активным игроком в тех областях, которые ранее считались прерогативой государств – в частности, в конце XX – начале XXI веков наметилась коммерциализация космоса, до этого доступного лишь государствам, в силу сложности и ресурсоемкости этой отрасли. Именно в результате деятельности крупного бизнеса происходит интернационализация высоких технологий между государствами. Ведущие транснациональные корпорации, базирующиеся в государствах-членах ОЭСР, финансируют развитие технологий в подразделениях, размещенных в развивающихся государствах, и более того, способствуют внедрению технологических инноваций. Научные сообщества, университеты и научно-исследовательские центры, внутригосударственные регионы, организации гражданского общества также выступают в роли акторов в международных научно-технологических отношениях. Все вышеописанные тенденции справедливы и для сферы информационных технологий (см. пп. 1.3).

«Развитие новых технологий, помимо тех очевидных выгод, которые оно приносит человечеству, создает новые и усугубляет существующие угрозы безопасности и устойчивому развитию, трансформирует природу и формы протекания международных конфликтов, порождает новые виды преступности и терроризма. Проблема обеспечения безопасности на национальном, региональном и глобальном уровнях, очевидно, приобретает качественно новое технологическое измерение. Несмотря на то, что высокотехнологичные угрозы международной безопасности не всегда исходят от государств, именно правительства играют ключевую роль в обеспечении международной стабильности, а поскольку большинство современных угроз носят глобальный характер, бороться с ними невозможно без принятия согласованных мер.

Развитие науки и технологий стимулирует расширение международного сотрудничества, причем формы и конфигурации участников этого сотрудничества становятся разнообразнее»[92]. Интенсификация международной кооперации обусловлена масштабностью новых вызовов, которые требуют объединения усилий нескольких государств[93]. В этих условиях наметилось создание новых международных режимов, направленных регулирование научно-технологической сферы. Однако, сотрудничество в сфере высоких технологий диктуется интересами государств, а негосударственные акторы, как правило, выполняют консультативные функции и лишь в ограниченной мере могут влиять на принятие итоговых решений.

Исследователи предлагают различные подходы к оценке современного этапа научно-технологического развития, однако большинство из них согласны с тем, что ИКТ играют ключевую роль в определении характеристик современного этапа развития, в том числе и в сфере международной политики. Так, академик РАН С.Ю. Глазьев полагает, что на современном этапе общество находится в рамках пятого технологического уклада, в рамках которого широкое

[92]Крутских А.В., Зиновьева Е.С. Информатизация и макротехнологии. Новое лицо мировой политики. // Международные процессы. 2014. № 36-37. С. 25.
[93] Kallerud E. Dimensions of Research and Innovation Policies to Address Grand and Global Challenges / Kallerud E., Klitkou A., Sutherland Olsen D., Scordato L. // NIFU, Oslo. 2013.

распространение получили пользовательские компьютеры, а также мобильные телефоны, что сделало возможным получать доступ в Интернет, и использовать связанные с этим пользовательские сервисы и технологические возможности[94]. Западные ученые используют термин NBIC для описания современного технологического уклада, что подразумевает конвергенцию четырех типов технологий: нано-, био-, инфо- и когно-технологий[95]. В настоящее время популярность приобретает концептуализация современного этапа технологического развития, опирающегося на возможности «интернета вещей» (под «интернетом вещей» понимается подключение интернету не только компьютеров и мобильных телефонов, но широкого спектра устройств, от бытовой техники до приборов медицинского назначения) в терминах «промышленной революции 4.0» (Industry 4.0). Данный подход пользуется особой популярностью в Германии. Автором концепции является К. Шваб, президент Всемирного экономического форума, который полагает, что повсеместное распространение устройств, подключенных к интернету, влечет за собой трансформацию промышленного производства, основанную на интеграции виртуальных и реальных производительных сил, что в свою очередь коренным образом изменяет все сферы жизни общества и государства (как это произошло, в свое время, в ходе других промышленных революций после появления парового двигателя, конвейера и массового производства, компьютеров и ЭВМ)[96]. В этих условиях происходит сочетание физического, цифрового и биологического миров, что оказывает синергетический эффект на современной общество, как сложную систему, трансформируя сложившиеся связи и отношения, в сфере экономики, политики, общественной жизни.

Революция в информационной произошла во второй половине XX века и составляла только одно измерение научно-технической революции, которая кроме

---

[94] Глазьев С.Ю. Уроки современной революции: крах либеральной утопии и шанс на «экономическое чудо». М.: «Экономическая газета», 2011. С. 330. (Цит по: Глобальная безопасность в цифровую эпоху: стратагемы для России / Под общ. ред. А.И. Смирнова М.: ВНИИгеосистем, 2014. С. 20.)

[95] См. напр.: Wolbring G. Why NBIC? Why human performance enhancement? //Innovation: The European journal of social science research. 2008. №. 1. P. 25-40.

[96] Шваб К. Четвертая промышленная революция. М.: ЭКСМО, 2017. 208 с.

информации включает в себя также развитие нано-, био- и когно-технологии. ИКТ являются наиболее распространенными. При этом они составляют основу для остальных технологий. Поэтому ИКТ оказывают существенное влияние на общество в целом, а, следовательно, и на отношения между государствами. Исследованиями влияния ИКТ на мировую политику занимаются теоретики информационного общества, чьи работы представлены в следующем параграфе, вместе с тем, влияние мировой политики на развитие ИКТ, в том числе в контексте их безопасного развития и использования, в международных исследованиях изучено мало. Настоящая работа восполняет данный пробел.

1.1.2. Теоретические основы анализа информационной революции в контексте международной политики и безопасности

Как правило, термины «постиндустриальное общество», «технотронное общество», «информационное общество», «сетевое общество», «общество знаний» используются как синонимы. Данные термины отражают различные сущностные характеристики информационного измерения современного этапа общественного развития.

В самом широком смысле «под информационным обществом понимают общество, ключевое значение в формировании, развитии и функционировании которого играет информация. Причем информация и используемые для ее передачи технологии определяют экономические, политические, культурные, социальные и иные значимые параметры информационного общества»[97]. Мировая политика в ходе последних нескольких десятилетий претерпела существенные изменения под воздействием на информационной революции.

Как правило, современная информационная революция трактуется как связанная с развитием ИКТ, а именно, компьютерных и телекоммуникационных технологий, а также постоянной динамической интеграцией этих технологий в

[97]Зиновьева Е.С. Вызовы и риски глобального информационного общества // Ежегодник ИМИ. Мировая политика: старые проблемы и новые вызовы. 2015. № 3. С. 119.

единую глобальную мультимедийную систему. Говоря о влиянии информационной революции на мировую политику, следует отметить, что еще в 1968 году советский философ А. Урсул выдвинул концепцию, согласно которой информация является одним из ключевых параметров объективного мира, определяющим процессы в рамках сложных адаптивных систем (каковой является и международная система).[98]На современном этапе академик К. Колин, развивая идеи А. Урсула, охарактеризовал информацию, как свойство всех систем живой и неживой природы, причем за счет обмена информацией между элементами системы происходят все эволюционные процессы в природе и обществе[99].

В западной литературе для обозначения изменений общественного развития, произошедших под влиянием информационной революции как правило используют термин «киберпространство». В науке о международных отношениях данный термин не обрел четкой формулировки. Р. Ридорн и Н. Чоукри на основании изучения научных и публицистических работ по данной проблематике пришли к выводу, что трактовка основных характеристик, а также оценка роли и места киберпространства в современной мировой политике варьирует в зависимости от теоретических предпочтений исследователей[100].

Как отмечает Д. Джакомелло, то же самое верно и для трактовок понятия «кибер-безопасность» и «информационная безопасность»[101]. В работах по международным отношениям, термин «киберпространство», как правило, связывают с процессами становления транснационального гражданского общества (Global Civil Society), влияния Интернет технологий на авторитарные режимы, вопросов управление Интернетом и кибербезопасности (cybersecurity).[102]

---

[98]Урсул А. Д. Природа информации: философский очерк. Политиздат, 1968. С. 288.

[99]Колин К. К. Философия информации и фундаментальные проблемы современной информатики //Almamater (Вестник высшей школы). 2010. №. 1. С. 29-35.

[100] Reardon R., Choucri N. The Role of Cyberspace in International Relations: A View of the Literature. 2012. // Paper Prepared for the 2012 ISA Annual Convention. San Diego, CA.1.04. 2012. URL: http://ecir.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf

[101] Security in Cyberspace: Targeting Nations, Infrastructures, Individuals. / Ed by G. Giacomello. Bloomsbury Publishing USA, 2014.256 p.

[102]Там же.

Подобная трактовка понятия информационного общества была распространена в западном исследовательском дискурсе вплоть до второй половины 2000-х гг.

Категория информации является ключевой в определении информационного общества, определения «информационного общества», предлагаемые различными теоретическими школами, существенно различаются. Так, известный американский социолог М. Кастельс понимает под информационным обществом общество, построенное по сетевому признаку, где ключевое значение имеет принадлежность к той или иной сети, к такой, например, как сети крупных транснациональных компаний или СМИ[103].

В 1990-е гг. была популярна теория А. Тоффлера о «третей волне», согласно которой развитие ИКТ является технологическим сдвигом, следующим после индустриальной революции, который может кардинально изменить технологический, экономический, политический и социальный уклад глобального общества.[104] Социолог, представитель критической школы М. Постер связывает современные медиа-структуры и общество постмодерна[105]. Согласно взглядам ученого неомарксистского толка Г. Шиллера, информационное общество по своей природе носит эксплуататорский характер, информация выступает в роли товара, который крупные медийные компании, базирующиеся в западных государствах, продают на невыгодных условиях населению развивающихся стран, укрепляя сложившиеся между развитым и развивающимся миром ассиметричные отношения зависимости.

Концептуализация и систематизация существующих направлений теории информационного общества разработаны Ф. Уэбстером в работе «Теории информационного общества»[106]. Ф. Уэбстер выделяет несколько подходов к определению информационного общества: экономический критерий, критерий, связанный со сферой занятости; пространственный критерий; критерий

[103] Castells M. The rise of network society. The Information Age: Economy, Society and Culture Vol. I. Malden, MA; Oxford, UK: Blackwell, 1996.
[104]Toffler A. Powershift: Knowledge, Wealth, and Violence in the 21st Century. N.Y.: BantamBooks, 1990 640 p.
[105]Poster M. The second media age. Blackwell, 1995. 200 p.
[106]Уэбстер Ф. Теории информационного общества. М.: Аспект-Пресс, 2005. 400 с.

культуры[107]. Рассмотрение различных подходов к определению информационного общества и выделению его ключевых характеристик позволяет прийти к выводу, согласно которому информационное общество в самом общем виде может быть определено как стадия развития общества, в рамках которой ИКТ оказывают значительное влияние на основные сферы жизни: экономическою, политическую и социокультурную.

При этом большая часть исследователей информационного общества методологически исходят из технологического детерминизма. Авторский подход к исследованию информационного общества и его влияния на международную безопасность характеризуется признанием взаимного влияния политики и технологий, в рамках которого значимые тенденции развития транснациональной политической среды[108] оказывают влияние на характеристики информационного общества, и наоборот, развитие ИКТ трансформирует современную мировую политику. Направления влияния информационной революции на современную мировую политику хорошо изучены в рамках междисциплинарных работ по теории информационного общества, основные выводы и подходы которых систематизированы ниже.

Несмотря на то, что распространение современных ИКТ и формирование информационного общества в целом носит повсеместный характер, уровень развития информационной инфраструктуры и ее доступности, а также степень включенности в глобальное информационное общество) разнится от государства к государству, что порождает противоречия и конфликтность на международной арене (отметим, что измерение уровня развития информационного общества в отдельной стране, как правило, проводится на основании развитости и доступности информационной инфраструктуры[109], однако, развитие инфраструктуры, как утверждают представители теории информационного

---

[107] Там же.

[108] Мельвиль А.Ю. Становление транснациональной политической среды и "волны" демократизации // Современные международные отношения и мировая политика: Учебник для вузов / Отв. ред. А.В. Торкунов; МГИМО(У) МИД России. – М.: Просвещение, 2004. – С. 106-142.

[109] См. напр. Measuring information society. 2014 Report. ITU, 2014. URL: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2014-SUM-PDF-R.pdf

общества, влечет за собой социо-культурные, политические и экономические трансформации, однако масштаб этих трансформаций варьирует от государства к государству).

Развитие Интернета не позволяет устранить анархичный и конфликтный характер современной международной системы. «Ответом на стремительный рост объёма мировой информации и глобализационные процессы является сегментация, в том числе в информационной сфере. Государственные, географические разграничения дополняют новые информационные границы. Такие государства, как Китай, Мьянма, Пакистан, Иран и др. ограничивают информационные потоки с помощью крупных Интернет-компаний, таких как «Google» и др., которые желают укрепить конкурентные позиции на перспективных рынках и поэтому передают органам государственной власти конфиденциальную информацию пользователей их услуг, блокируют доступ к определенным сайтам»[110]. Появление подобных «цифровых границ» связано с легкостью доступа к информации в современном мире, что создает возможности воздействия на общественное мнение поверх государственных границ. Таким образом, помимо информационной инфраструктуры важным объектом информационного воздействия является индивидуальное и массовое сознание.

Информатизация является ключевой характеристикой современности. Соответственно, уровень развития государства и его положение на международной арене в значительной степени обусловлены уровнем информатизации. Развитые и развивающиеся страны существенно отличаются по степени развития и внедрения ИКТ, это явление получило название «цифровой разрыв». Таким образом, политическое лидерство в мире предполагает и информационное лидерство. Следует при этом различать использование ИКТ и информатизацию общественных отношений. Несмотря на то, что информационное общество возникает в рамках отдельных государств с разной степенью интенсивности, но в соответствии с общими закономерностями – одной

[110]Зиновьева Е.С. Роль международных организаций и институтов в формировании режима управления интернетом. Дис. на соискание ученой степени кандидата политических наук. М.: МГИМО, 2009. С. 5.

из которых является возрастающая зависимость от ИКТ, что актуализирует проблему информационной безопасности, как на уровне отдельных государств, так и на международном уровне (так как нормальная работа электронно-вычислительных комплексов, автоматизированных систем и отдельных компьютеров без преувеличения имеет жизненно важное значение). Как отмечает швейцарский экономист, основатель Всемирного экономического форума К. Шваб, основная опасность современного этапа технологического развития заключается в его реализации на основании принципа «победитель получает все», что усугубляет социальное напряжение и конфликты, в том числе международные, способствует дестабилизации международной обстановки, особенно в условиях, когда ИКТ позволяют людям получать оперативную и достоверную информацию о социальной несправедливости и несоответствиях в условиях жизни государств.

С развитием и внедрением ИКТ изменяются критерии военной мощи государства, которая включает в себя информационную составляющую. Однако, в политическом плане значение современной информационной революции шире. Информация и ИКТ выступают в роли важной составляющей т.н. «совокупной мощи» государства. По выражению Г. Моргентау, «международная политика, как и любая другая есть борьба за власть»[111]. При этом власть и влияние на международной арене зависят от контекста (так, в работах реалистов можно проследить эволюцию понимания силы государства – если для представителей классического реализма сила выражалась в показателях военной мощи[112], то для неореалистов характерно включение экономического потенциала в категорию совокупной мощи государства[113]).

ИКТ не являются независимым агентом изменений, определяющим ключевые характеристики современного общества и мировой политики. Как и любые другие технологии, они вписаны в более широкий социальный, политический, экономический контекст и является отражением происходящих в

[111]Morgenthau H. Politics among nations: the struggle for peace and power. 1973. P. 82.
[112]Там же. P. 84
[113] Waltz K. N. Theory of international politics. Waveland Press, 2010. 256 p.

обществе, в том числе и на международном уровне, процессов. Возрастающая в последние годы конфликтность в международной системе отражается ростом напряженности в глобальном информационном пространстве. Как отметил Президент России В.В. Путин на заседании коллегии ФСБ в марте 2015 г., в 2014 г. было пресечено около 74 миллионов атак на официальные сайты и информационные системы органов власти России[114].

1.2. Развитие информационного общества в контексте мировой политики

1.2.1. Интернет как основа информационного общества: тенденции развития

Как уже было показано в предыдущей главе современный этап развития ИКТ оказывает существенное влияние на мировую политику и международную безопасность. Особое место среди распространенных сегодня ИКТ занимает глобальная сеть Интернет.

Развитие Интернета формирует глобальное информационное пространство. Под глобальным информационным пространством в настоящей работе понимается «электронная среда, посредством которой информация создается, передается, принимается, хранится, обрабатывается и уничтожается»[115], а также собственно информация и знания, которые обращаются в рамках этой среды. Таким образом, глобальное информационное пространство не исчерпывается сетью Интернет, в него входят как другие информационные сети, так и информация, и знания, создаваемые, хранимые, обрабатываемые и передаваемые посредством этих сетей. Однако именно Интернет представляет собой основную инфраструктуру информационного общества и характеристики, присущие

[114] В.В. Путин. Выступление на заседании коллегии ФСБ. 26.03.2015 URL: http://nod66.ru/2015/03/26/10194/
[115] Rauscher K. F., Yaschenko V. Russia–US Bilateral on Cyber Security: Critical Terminology Foundations //New York, USA: East West Institute. 2011.URL: https://www.files.ethz.ch/isn/130080/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20(2)-1.pdf

Интернету, оказывают влияние на природу глобального информационного пространства и обеспечение информационной безопасности.

Итальянский философ, профессор Оксфордского университета, Л. Флорриди сформулировал концепцию, в рамках которой, человек рассматривается как информационный объект, который в процессе своей жизнедеятельности взаимодействуют с другими информационными объектами (под которыми понимаются любые объекты живой и неживой природы)[116] Все информационные объекты существуют в рамках «инфо-сферы» или «информационного пространства», которое представляет собой среду, где происходит обмен данными, информацией и знаниями. Физическим воплощением глобального информационного пространства, как среды международного взаимодействия людей — информационных объектов, а значит и ядром происходящих там процессов является сеть Интернет.[117]

Значимость Интернета как ключевой инфраструктуры глобального информационного общества подтверждается масштабами его использования. Число пользователей Интернета постоянно увеличивается – если в начале 2008 г. насчитывалось 1.4 млрд. пользователей, то в 2017 г. уже3.7млрд., то есть почти половина всего населения мира[118]. В России в 2016 г. Интернетом пользовалось 67% взрослого населения страны (старше 12 лет) – то есть около 83млн. человек [119]. С 2000 г. число активно использующих Интернет людей выросло на 936%[120].

Для понимания тех изменений, которые процессы информатизации привносят в международную систему, а также специфики международных отношений в области обеспечения информационной безопасности и управления Интернетом необходимо обозначить ключевые характеристики Интернета, а также перспективные направления развития глобальной сети.

---

[116]Capurro R. On Floridi's metaphysical foundation of information ecology //Ethics and information technology. 2008. №. 2-3. С. 167-173.

[117]Там же.

[118]Internet World Stats. Usage and population statistics. URL:www.internetworldstats.org

[119] Развитие интернета в регионах России. Весна 2016. // Исследование Яндекс. URL: https://yandex.ru/company/researches/2016/ya_internet_regions_2016

[120]Internet World Stats. Usage and population statistics. URL:http://www.internetworldstats.com/stats.htm

Интернет представляет собой сложную и неоднородную макросистему, объединяющую значительное количество информационных сетей. Технологический дизайн позволяет обеспечить нейтральность технологии, которая объединяет множество локальных сетей (т.н. «Сетевая нейтральность»), что и делает Интернет ключевой инфраструктурой в рамках глобального информационного общества.

Создание интернета принято датировать 1969 г., когда впервые были объединены в единую сеть четыре компьютера в ходе научно-исследовательской программы Министерства обороны США. В 1972 г. базовые протоколы интернета TCP/IPбыли приняты в качестве основных стандартов передачи данных, а в 1983 году – появилась система доменных имен и первые вирусы, а свой современный облик интернет приобрел в 1989 году, когда была создана всемирная паутина как сеть связанных гиперссылками страниц, по которым можно перемещаться с помощью графического интерфейса[121].

Большая часть современных гигантов Интернет-индустрии, такие как Facebook, Twitter, была образована в 2000-х гг. Эти компании позволяют пользователям Интернета общаться, обмениваться персональной информацией: текстами, фотографиями, видео[122]. Пользователи самостоятельно генерирую контент и зачастую составляют конкуренцию многим медийным корпорациям, что формирует модель коммуникации «многие-ко-многим».

На сегодняшний день охват Интернета глобален, при этом наибольшее число пользователей проживает в Азии (49.8% от общего числа, всего более 1 млрд.), на втором месте Европа (17% от общего числа), на третьем Латинская Америка и государства Карибского бассейна (10% от общего числа), на четвертом Африка (10% от общего числа) и лишь на пятом Северная Америка (8% от общего числа).. Статистические данные показывают меняющуюся геополитику современного информационного пространства – все более влиятельными центрами силы в информационной сфере становятся незападные государства.

---

[121]IP разбивает информацию на пакеты, TCP контролирует, что они полностью получены адресатом.

[122]Эванс Д. Интернет вещей: как изменится вся наша жизнь на очередном этапе развития Сети: официальный сайт компании Cisco. URL:http://www.cisco.com/web/RU/news/releases/txt/2011/062711d.html

Для понимания Интернета как явление необходимо дать характеристики текущих тенденций его развития.

1. Количественный рост пользователей Сети происходит в основном за счет Азии и Ближнего Востока. Отражением этого процесса является тот факт, что наиболее распространенным языком в Сети является китайский[123]. Россия также старается продвигать русский язык в Интернете. Прежде всего в этих целях в 2010 г. был создан домен на кириллице «.рф». Этим путем идут многие страны, в результате чего Интернет со временем неизбежно станет многоязычным.
2. Благодаря повсеместному распространению мобильной связи Интернет также становится повсеместным, происходит формирование Web 3.0 – всеобщей Сети. Уже сегодня мобильный Интернет по числу пользователей превосходит стационарный Интернет. Мобильные соединения предполагают динамичные IP-адреса (пользователь получает новый адрес с каждым новым соединением), хотя изначально Интернет задумывался как стационарная система со стационарными адресами.
3. Продолжает расти блогосфера и peer-to-peer сети. При этом видеоблоги становятся более популярны, чем текстовые или графические блоги. Уже в 2009 г. число пользователей социальных сетей превысило количество пользователей электронной почты. К настоящему моменту число пользователей Facebook превысило 1 млрд, причем наиболее быстрый рост данного сегмента Интернета приходится на Индию, Бразилию, Россию, Ближний Восток и Африку. Кроме глобальных социальных сетей активно развиваются и национальные сети, такие как российская VK, китайская QQ[124].
4. Обретает устойчивость тенденция к объединению различных телекоммуникационных технологий и формирование унифицированной коммуникаций. Объединяются такие технологии как телефония, телевидение, радио и др. на основе сетей, основанных на пакетной передаче данных.

[123]Internet World Stats. Usage and population statistics. URL:www.internetworldstats.org
[124]Top Sites. Alexa Rank. The top 500 sites on the web. URL: http://www.alexa.com/topsites

5. Распространяются «облачные» технологии хранения и обработки данных. Это позволяет получить максимальную отдачу от существующих компьютерных возможностей. Информационные ресурсы отдельных пользователей все чаще хранятся в так называемых «серверных фермах». Облака создают и предоставляют для размещения данных такие гиганты информационного рынка, как Google, Apple, Microsoft, Amazon и Facebook. В результате Интернет приобретает действительно трансграничную архитектуру.
6. Важным трендом последнего времени в развитии Интернета стало повышение значения «больших данных». Этот термин обозначает сверхкрупные массивы данных. Потенциально такие данные могут существенно повысить эффективность управления социальными процессами (в том числе политическими) на микроуровне, т.е. на наиболее фундаментальном уровне общества. Пока современные технологии позволяют только накапливать эти серверы большие массивы данных, однако эффективно обрабатывать их пока не научились.
7. Быстро развивается «Интернет вещей», в рамках которого к Интернету подключаются не только пользователи при помощи компьютеров и мобильных телефонов, но и различные физические устройства. Согласно прогнозу консалтинговой компании «Международная корпорация данных», к 2020 году к Интернету вещей будет подключено 212 миллиардов устройств, а объем этого рынка составит $8,9 трлн[125]. По оценкам экспертов, приведенным в работе президента Всемирного экономического форума К. Шваба, в обозримом «будущем каждое физическое изделие можно будет подсоединить к единой инфраструктуре связи и повсеместные датчики позволят людям»[126] существенно повысить качество жизни.
8. Растущее экономическое значение имеет технология цепочки блоков транзакций (block chain) и криптовалюты (как, напр. Bitcoin). «Bitcoin и другие криптовалюты основаны на механизме распределённого доверия под названием «цепочка блоков транзакций (block chain) – способа отслеживать доверенные системе транзакции

[125] The Internet of Things Is Poised to Change Everything, Says IDC // Business Wire. 03.10.2013. URL: http://www.businesswire.com/news/home/20131003005687/en/Internet-Poised-Change-IDC#.VdE-Vfmqqko
[126] Шваб К. Четвертая промышленная революция. М.: Издательство «Э», 2017. С. 159.

определенным способом»[127]. К достоинствам технологии цепочки блоков транзакций можно отнести ее устойчивость и высокий уровень безопасности от кибермошенничества (внедриться в цепочку блоков достаточно в силу особых механизмов шифрования). Кроме того, криптовалюты не подвержены инфляции. Общая стоимость всей криптовалюты Bitcoin, обращающейся сегодня, составляет 0.025% от мирового ВВП[128].

9. Развитие систем искусственного интеллекта. Современные системы искусственного интеллекта способны извлекать уроки из прошлых ситуаций для того, чтобы обеспечивать входящую информацию и автоматизировать процесс принятия решений, облегчая и ускоряя получение конкретных выводов на основании собранных данных и прошлого опыта, в том числе при помощи обработки «больших данных». Искусственный интеллект на сегодняшний день позволяет создавать самоуправляемые системы для вождения автомобилем, а также используется для решения ряда задач в военной и гражданской сферах[129].

На современном этапе развитие социальных медиа и формирование Web 2.0 стало значимой тенденцией, определяющей облик Интернета и глобального информационного пространства в целом. Термин Web 2.0 был предложен Т. О'Рейли в 2003 году[130]. О'Рейли выделил 7 ключевых принципов, на которых основан новый этап в развитии всемирной сети: Интернет становится ключевой платформой политического дискурса; использование Интернета в политических целях формирует коллективное самосознание пользователей сети; значимость данных превышает значимость программного обеспечения и технической инфраструктуры; быстрая трансформация публичной политики в результате использования социальных медиа; распространение политического контента с помощью различных приложений, обширный пользовательский эксперимент на политических сайтов[131].

---

[127] Там же. С. 180.
[128] Там же.
[129] Там же.
[130] O'Reilly T. What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software. // Oreilly.com 30.09.2005 URL: http://oreilly.com/web2/archive/what-is-web-20.html
[131] Stayner J. Web 2.0 and the transformation of news and journalism // Handbook of Internet Politics. / Ed by A. Chadwick, London: Routledge, 2008. P. 212

«Интернет усиливает многие значимые тенденции и процессы современной мировой политики, в том числе глобализацию, размывание государственных границ, взаимозависимость в экономической сфере, выход негосударственных акторов на мировую арену. Одним из негативных последствий глобальной информатизации стало ее влияние на межгосударственное противоборство, которое переходит в цифровую среду, порождая такой феномен как информационные войны и конфликты, а также кибершпионаж. Террористическая и преступная деятельность также дополнилась новым арсеналом средств информационного воздействия, порождая угрозы национальной и международной безопасности»[132].

Как и любая другая технология, ИКТ и сформировавшееся на их основе информационное общество по своей сути тесно связаны с политикой, так как определение ключевых характеристик технологий является предметом политических противоречий, в том числе на международном уровне. Транснациональная природа информационного пространства, а также ряд иных его характеристик и перспективных тенденций развития, диктует необходимость международного взаимодействия, в том числе с целью обеспечить международную безопасность в данной области.

1.2.2. Регионализация глобального информационного пространства

В последние годы в исследовательской литературе все чаще отмечается тенденция к «балканизации» интернета, его локализации[133] вследствие выделения суверенных сегментов глобальной сети отдельными государствами, как правило, по соображениям обеспечения информационной безопасности. Вместе с тем, тенденция к локализации является частью более широкой тенденции к регионализации глобального информационного пространства.

---

[132] Там же.

[133] См. напр.: Cavelty M. The Resurgence of the State: Ttrends and Processes in Cyberspace Governance / M.Cavelty, M.Dunn, S.Krishna-Hensel, V.Mauer. Asghate: Ashgate Publishing, Ltd., 2007. 165 p.

Тенденции развития глобального информационного пространства в определенной степени повторяют тенденции развития других телекоммуникаций, прежде всего, международной телеграфной и телефонной сети (при этом, следует учитывать, что любые аналогии носят лишь ограниченный характер и об абсолютно идентичных тенденциях речи не идет). Подобное исследование позволит вписать современный этап развития Интернета в более широкий исторический контекст

Во второй половине XX века международная телефонная сеть в рассматриваемый период выступала в качестве основного канала международной коммуникации, так же как и Интернет на современном этапе. Тенденции распространения информации в глобальной телефонной сети отражали трансформации структуры международных отношений. Если в годы холодной войны телефонная система представляла собой две слабо связанные подсистемы, расположенные внутри блоков соперничающих государств, то после окончания холодной войны она образовала единую глобальную систему с центром потоков, распложенным в США, а затем в начале 2000-х по мере формирования многополярной международной системы потоки телефонного траффика также стали тяготеть к регионализации, сформировав несколько связных подсистем, причем основная из них находилась в США.

Можно сделать вывод, что направленность телекоммуникационных потоков информации внутри телефонной сети отражала природу международных отношений. Так, в период с 1980 по 2000 гг. происходили процессы экономической, а затем и политической глобализации, причем после распада СССР США оказываются лидером, и в этих условиях сформировалась международная телекоммуникационная система, где США выступали центром мировых экономических и политических процессов, и как следствие центром международных коммуникаций.[134] В 2000-х гг. снижение возможностей США по управлению глобальными процессами и тенденция к формированию

[134]The political economies of media: The transformation of the global media industries / Ed by D. Winseck .Bloomsbury Publishing, 2011.

многополярной системы международных отношений привело к изменению направленности международных телефонных звонков, их внутри региональной ориентации. Вследствие финансово-экономического кризиса, а также ряда проблем, с которыми столкнулись США и страны ЕС в международной политике, и, следовательно, в глобальной телекоммуникационной сети и в Интернет-пространстве, тенденция к регионализации усилилась. Это было обусловлено, с одной стороны кризисом неолиберальной модели глобализации, а с другой усилением региональных центров силы.[135]

«В потоках мирового Интернет-трафика (рассчитанного на основании анализа передачи пакетов данных по открытым сетям)США остается центральным информационным хабом. США также занимают ключевое место как центральный узел глобальной кабельной инфраструктуры интернета[136]. Вместе с тем интенсифицируются информационные потоки между культурно и территориально близкими государствами (можно выделить Латино-Американский сегмент глобального информационного пространства интернета, сегмент из группы стран Юго-Восточной Азии (с очень большим количеством смежных взаимосвязей), сегмент постсоветских государств, где значительное количество населения говорит на русском языке, Евроатлантический сегмент (который остается ключевым), при этом в перспективе можно ожидать, что интенсифицируются потоки интернет-коммуникации между государствами ШОС и БРИКС, что обусловлено, прежде всего, политическими причинами и стремлением государств создать альтернативный проект Интернета[137] (однако, пока рано говорить о формировании единой информационной системы, так как культурные и языковые различия препятствуют коммуникации на уровне обществ). Такая структура международной передачи данных отражает характер развития глобального информационного пространства, где США выступали государством, инициировавшим инновации в технологической, экономической и

[135]The political economies of media: The transformation of the global media industries. / Ed by Winseck D. Bloomsbury Publishing, 2011.
[136]См. статистику Oxford Internet Institute. URL: http://geography.oii.ox.ac.uk/?page=home
[137] Страны БРИКС создадут независимый от США Интернет // Новости RT на русском. 29.10.2013. URL: http://russian.rt.com/article/17519

политической составляющих глобальной информационный системы, что подразумевает более высокий уровень развития Интернет технологий и центральную роль в глобальной информационной системе. При этом в настоящее время США частично утрачивают лидирующие позиции в рамках глобального информационного пространства»[138].

Особую роль в регионализации информационного пространства играют сложившиеся устойчивые схемы взаимодействия пользователей в ходе поиска информации в сети (то есть работу с информационным содержимым Интернета – контентом). Речь идет о паттернах использования общих веб-сайтов, в качестве источников информации в разных странах (сегодня наиболее популярными сайтами среди пользователей интернета являются поисковые системы, социальные сетевые сервисы и почтовые сервисы). Главным фактором, определяющим предпочтения пользователей Интернета в отношении контента, является культурная и языковая близость, без которой труднодостижимо формирование единого информационного пространства в регионе. Если говорить о совместном использовании социальных сетей, то следует отметить, что на современном этапе Facebook является наиболее распространенной сетью, однако в регионе постсоветского пространства активно используются такие сети, как Вконтакте и Одноклассники, а Китай вместе с Гонконгом в основном используют национальную социальную сеть QQ. При этом связи Китая с Россией в данном измерении не столь значимы. Также можно выделить информационную подсистему внутри глобального Интернета, в которую входят пользователи из арабских стран, среди которых Саудовская Аравия, Египет, Алжир, Кувейт, Катар, Объединённые Арабские Эмираты[139]. Таким образом, информационные кластеры в интернете, которые, в силу своей культурной и религиозной идентичности, несколько обособленные от глобального информационного пространства. «Население стран в рамках одного кластера использует одни и те же сайты для получения информации, общения и пр., что отражается на

[138]Стратегическое прогнозирование международных отношений. Коллективная монография. / Под ред. А.И. Подберезкина, М.В. Александрова. М.: МГИМО, 2016. С. 337.
[139]См. статистику Oxford Internet Institute. URL: http://geography.oii.ox.ac.uk/?page=home

мировоззрении и самоидентификации населения данных стран. В определенной степени данная тенденция к регионализации обусловлена политическими причинами, а именно, стремлением обособиться от глобального информационного пространства, сохранив собственную идентичность в условиях глобальной информатизации. Кроме того, определенное влияние оказывают языковые различия и ограничения на использования американских социальных медиа в отдельных государствах, которые рассматриваются как каналы распространения «мягкой силы» и влияния США»[140].

В первую очередь следует отметить, что глобальное информационное пространство, первоначально сформировалось как единая система с центром информационных потоков и инфраструктуры в США, однако по мере развития Интернета информационное пространство во все большей степени начинает приобретать характеристики, свойственные международной политике. Формируются региональные подсистемы информационного пространства. Так, среди основных подсистем глобального информационного пространства можно выделить следующие: страны постсоветского пространства, страны, говорящие на китайском языке и страны с большим количеством китайских мигрантов, а также кластер, состоящий из арабских стран. С точки зрения инфраструктуры Интернета, структурирование выглядит несколько иначе – в рамках глобального американо-центричного информационного пространства выделяют Латино-Американский сегмент, сегмент стран Юго-Восточной Азии, постсоветский сегмент, Евроатлантический сегмент, при этом интенсифицируются инфраструктурное взаимодействие между государствами БРИКС и ШОС.

«Таким образом, тенденция к регионализации, характерная для современной международной политики и мировой экономики[141] характерна также и для информационного пространства. Регионализация происходит как часть более широкой тенденции к «балканизации» Интернета, выделению сегментов

---

[140]Стратегическое прогнозирование международных отношений. Коллективная монография. / Под ред. А.И. Подберезкина, М.В. Александрова. М.: МГИМО, 2016. С. 338.

[141]См. напр.: UNCTAD World investment report 2014 Investing in the SDGs: an Action Plan. UNCTAD/WIR/2014.Geneva, 2014. URL: http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=937

сети с целью защиты «информационного суверенитета», что обусловлено, с одной стороны, сохраняющимися межгосударственными противоречиями, а с другой стороны, стремлением обеспечить информационную безопасность и извлечь коммерческую выгоду из развития Интернет-технологий»[142].

Тенденция к регионализации информационного пространства во многом связана с выявленной М. Кастельсом закономерностью современного этапа развития глобального информационного общества, основанного на сетевых структурах, в рамках которого основным противоречием является противоречие между глобализацией и стремлением отдельных сообществ сохранить свою идентичность[143], что в свою очередь актуализирует проблему информационной безопасности.

На современном этапе международная политика становится определяющим фактором развития информационного пространства (по выражению Г. Моргентау «международная политика, как и любая другая, есть борьба за власть»[144]). Вместе с тем, как было показано ранее, любая технология находится в сложном взаимодействии со средой, и направления технологического развития могут оказывать влияние на социальные отношения, с чем связано появление новых и усиление существующих тенденций в мировой политики в условиях глобальной информатизации (взаимозависимость, рост влияния негосударственных акторов, «размягчение» государственного суверенитета»).

1.2.3. Управление Интернетом в контексте международной безопасности

Характеристики Интернета и системы управления им оказывают влияние не только на международно-политический ландшафт глобального информационного пространства, но на международную информационную безопасность. С точки

[142]Стратегическое прогнозирование международных отношений. Коллективная монография. / Под ред. А.И. Подберезкина, М.В. Александрова. М.: МГИМО, 2016. С. 337.
[143] Кастельс М. Могущество самобытности // Новая постиндустриальная волна на Западе. Антология / Под ред. В.Л. Иноземцева. М.: Academia, 1999.
[144] Morgenthau H. Politics among nations: the struggle for peace and power. 1973. P. 82.

зрения стабильности и безопасности развития и использования Интернета и международной информационной безопасности в целом, важнейшее значение имеет сложившаяся система международного управления Интернетом, а также роль ведущих государств и негосударственных акторов в данной системе.

В соответствии с определением, представленным в итоговом отчете Рабочей группы по вопросам управления Интернетом ООН «управление Интернетом представляет собой разработку и применение правительствами, частным сектором и гражданским обществом, при выполнении ими своей соответствующей роли, общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение Интернета»[145].

США финансируя работы по созданию Интернета, участвовали и в определении характеристик управляющих структур, что и объясняет их лидирующее положение в рамках современного режима управления всемирной сетью. Так, Интернет был создан в рамках работ Агентства перспективных разработок (Advanced Research Project Agency, ARPA) Министерства обороны США.

По мере роста количества пользователей, коммерческого потенциала новой технологии, государства, как развитые, так и развивающиеся, стали стремиться усилить свое влияние в данной области, в том числе принимая внешнеполитические усилия, направленные на интернационализацию управления интернетом. Эти процессы нашли отражения в научных трудах. Одними из первых исследователей, обративших внимание на то, что на создание кода, лежащего в основе глобальной сети Интернет, влияют государства и крупный бизнес, стали Л. Лессиг[146] и М. Мюллер[147]. Отсутствие регулирования со стороны правительств и международных организаций рассматривалось авторами как угроза стабильному функционированию Интернета и безопасности пользователей. Однако по мере развития интернета увеличивался и масштаб

[145]Доклад рабочей группы по управлению Интернетом. Шато де Босси, 2005. URL:http://www.wgig.org/docs/WGIGReport-Russian.pdf
[146]Lessig L. Code and other laws of cyberspace. – NY: Basic books, 1999.
[147] Mueller M. Ruling the root: Internet governance and the taming of cyberspace. MIT press, 2002.

государственного регулирования данной технологии, так же, как и предшествующих ему ИКТ, таких как телеграф, телефон, радиовещание и т.п. Государства начали создавать правила, которые управляют поведением пользователей и развитием Интернета. Одним из первых шагов на пути к формированию системы управления Интернетом было создание ICANN.

Инициативы правительства США, направленные на коммерциализацию Интернета, предшествовавшие созданию ICANN (а именно, передача функций управления технической инфраструктурой интернета коммерческой структуре), спровоцировали протест как со стороны широкой общественности (прежде всего, пользователей интернета), так и представителей государств. В целях сохранения контроля над ключевыми элементами инфраструктуры Интернета, правительство США приняло решение передать функции управления системой доменных имен (Domain Name System, DNS)[148] некоммерческой организации, с целью оградить Интернет от правительственного влияния (за исключением правительства США, которые сохраняли контрактные отношения с создаваемой организацией). В ноябре 1998 г. создание ICANN было оформлено Меморандумом о взаимопонимании между ICANN и Министерством торговли США.

ICANN была создана и официально функционирует как неправительственная организация, зарегистрированная в США. Работа ICANN регулируется Законом штата Калифорнии о некоммерческих юридических организациях, созданных с целью осуществления благотворительной и общественной деятельности[149].

Изначально функции ICANN включали в себя т.н. “IANA (Internet Assigned Numbers Authority) functions”:

- координацию работ по выработке технических параметров Интернет-протоколов;
- административные функции по управлению базами данных корневого сервера системы доменных имен (в т.ч. создание новых доменов верхнего уровня);

[148]DNS (англ. Domain Name System — система доменных имён) — распределённая система (распределённая база данных), способная по запросу, содержащему доменное имя хоста (компьютера или другого сетевого устройства), сообщить IP-адрес, или (в зависимости от запроса) другую информацию.

[149]Ответственность и прозрачность ICANN: структура и принципы // Принципы управления ICANN. Октябрь 2007. URL:http://www.icann.org/en/transparency/acct-trans-frameworks-principles-russian-17oct07.pdf

- распределение блоков IP-адресов.

Соглашение между ICANN и Министерством торговли США в последний раз было пересмотрено 30 сентября 2016 года, давало этому государственному ведомству полномочия по контролю над деятельностью ICANN и участию в ней. На сегодняшний день функции IANA были переданы В 2016 году была предпринята очередная реформа ICANN. Функции управления адресным пространством сети были переданы дочерней организации ICANN Public Technical Identifiers (PTI). Данная организация формально независима от Министерства торговли США (то есть для внесения изменений и в базу данных корневой зоны в целом выполнения своих административных функций ей не требуется формального одобрения со стороны Министерства торговли США), но при этом зарегистрирована в США, штат Калифорния и не имеет права выводить критические инфраструктуры адресного пространства интернета за пределы штата[150]. Большая часть Совета директоров организации была назначена ICANN, все они – представители развитых государств. Решения в рамках PTI принимаются на основании многоуровневой модели, в которой право голоса имеют государства, организации гражданского общества, бизнес, эксперты. Более того, само существование PTI будет зависеть от продления контракта с ICANN, по отношению к которой она выполняет функции субподрядчика; работа PTI будет прекращена в том случае, если Министерство торговли США расторгнет контактные отношения с ICANN[151]. Таким образом, вышеназванная реформа не решает проблем с легитимностью существующей модели управления интернетом, оставляя правительству США весьма существенные рычаги влияния.

Более того, как отмечает И. Щеголев, помощник Президента Российской Федерации, создание PTI потенциально порождает новые проблемы: ««До этого хотя бы можно было предъявить претензии правительству США, если что-то происходило. А сейчас это некая автономная или некоммерческая организация, которая просто работает по американскому праву. И американские чиновники

[150]IANA Naming Function Contract. 30 September 2016. URL: https://www.icann.org/iana_pti_docs/151-iana-naming-function-contract-v-30sep16
[151] Там же.

могут сказать: «Мы здесь ни при чем. Идите в суд в Калифорнии и судитесь с этими ребятами»[152]. Таким образом, Россия не признает эффективность и легитимность текущего институционального дизайна управления ключевыми техническими ресурсами интернета и намерена в рамках международных переговоров добиваться интернационализации этих функций и передачи их к Международному союзу электросвязи, где одна страна имеет один голос и решения принимаются на основании межправительственной модели.

Как показывает М. Карр, сотрудник Департамента международной политики Университета в Аберсвитте, Великобритания, распространение многосторонних моделей управления Интернетом в основном служит задаче усиления существующих властных отношений на международной арене, а не их разрушению. Более того, многоуровневая модель управления Интернетом ставит в привилегированное положение тех акторов, которые стояли у истоков сети – а именно, США и тех государств, чьи интересы находятся в одном ключе с внешнеполитической повесткой дня, продвигаемой США[153].

Следует подчеркнуть политическое измерение IANA функций. Техническая координация обеспечивает возможность принятия решений, традиционно относимых к сфере государственной политики, таких как управление интеллектуальной собственностью, рыночной структурой индустрии распределения доменных имен, защита прав отдельных пользователей сети, в частности обеспечение неприкосновенности частной жизни.

Таким образом, ICANN контролировала (и продолжает косвенно контролировать посредством отношений с PTI) оспариваемые и экономически значимые технические ресурсы (в частности доменные имена), что объясняет взаимосвязь выполняемых ею функции технической координации с целым набором очень важных задач из области внутренней и международной политики.

---

[152] Россия будет добиваться изменения системы управления интернетом в мире // РБК 27.03.2017. URL: http://www.rbc.ru/technology_and_media/27/03/2017/58d508179a7947d969c13c50

[153] Carr M. Power Plays in Global Internet Governance //Millennium-Journal of International Studies. 2015. Т. 43. №. 2. P. 640-659.

Однако, ICANN и PTI стремятся к деполитизации своей роли в управлении Интернетом и обеспечении информационной безопасности, с тем, чтобы вывести данную проблема из сферы международного обсуждения.

Не раз высказывались опасения, что правительство США может использовать ICANN и PTI для реализации своих внешнеполитических целей. Функции IANA предполагают возможность удаления записи о доменах враждебных США государств из базы данных корневого сервера. Несмотря на то, что формально PTI независима от правительства США в процессе принятия решений, она является дочерней структурой ICANN, которую связывают с правительством США т.н. «особые отношения», описанные выше. В международно-политическом ключе роль правительства США в реализации IANA функций вышла на передний план в ходе принятия решения о создании доменов .ps (Палестинская территория) и .tw (Тайвань), которые расцениваются многими как потенциальные причины конфликтов.

Подводя итог, можно сказать, что при всей политической значимости принимаемых решений PTI, как ранее ICANN, не нашла поддержки у международного сообщества.

Дебаты в отношении легитимности ICANN шли с момента ее создания и продолжаются до сих пор, теперь уже в отношении PTI. Критика ведется по следующим основным направлениям:

- критика односторонней политики США в отношении контроля над системой корневых серверов;
- недовольство институциональной структурой PTI, в рамках которого правительства обладают лишь консультативными полномочиями;
- общее восприятие PTI как организации, в недостаточной степени учитывающей интересы развивающихся стран.

Вся история международных переговоров по вопросам международного управления интернетом, которые вошли в свою активную фазу начиная с 2003 года, в ходе Всемирного саммита по вопросам информационного общества (ВВУИО) подтверждает недовольство большинства стран мира односторонними

возможностями влияния США в рамках современного режима управления интернетом.

Всемирный саммит по вопросам информационного общества прошел в два этапа – в Женеве в 2003 г. и в Тунисе в 2005 г. Во время саммита вопросы управления Интернетом впервые вышли на передний план международной повестки дня. В ходе саммита вопрос о реформе ICANN вызвал ожесточенные споры. Основным итогом международных переговоров по вопросам управления Интернетом в ходе ВВУИО создание совещательного Форума по управлению Интернетом (ФУИ). ФУИ предназначен в первую очередь для обсуждения в многостороннем формате проблем, связанных с управлением Интернетом, это в большей степени площадка для дискуссий, чем инструмент для принятия политических решений.

«В декабре 2012 года в Дубаи прошла Всемирная конференция по международной электросвязи, ставшая важной вехой в череде дискуссий об управлении Интернетом на глобальном уровне. Россия на конференции занимала проактивную позицию, предложив ряд существенных изменений в международный режим управления Интернетом. В частности, Россия предложила рассматривать Интернет как новую глобальную инфраструктуру электросвязи по аналогии с другими, такими, например, как телефонная сеть. Это означает, что Интернет, как и иные сети, следует регулировать на межгосударственном уровне, а государственный суверенитет распространить на национальные сегменты Интернета. Российские инициативы были поддержаны Китаем, рядом арабских государств, а также странами Центральной Азии»[154].

Самым активным противником конференции в Дубае выступила компания Google, на сайте которой был объявлен сбор подписей за свободный Интернет. «США отказались поддержать инициативы по усилению международной составляющей регулирования Интернета, обосновав свою позицию стремлением

[154]Зиновьева Е.С. «Цифровой Вестфаль»? [Электронный ресурс] // Эксперты МГИМО. 26.03.2013. URL: /news/experts/document236588.phtml

избежать угроз для свободы Интернета[155]. По итогам конференции международный режим управления Интернетом существенных изменений не претерпел»[156].

Дополнительный импульс переговорному процессу придали разоблачения Эдварда Сноудена, включая раскрытие фактов электронного шпионажа в глобальном масштабе со стороны США. 23-24 апреля 2014 г. в г. Сан-Паулу, Бразилия состоялась Глобальная встреча заинтересованных сторон по вопросам будущего управления Интернетом (NETmundial). Работа встречи была направлена на «выработку принципов управления Интернетом и составление предложения о дорожной карте дальнейшей эволюции экосистемы управления Интернетом»[157]. Созыв встречи стал результатом недовольства партнеров США тем фактом, что США, несмотря на неоднократные заявления об открытости Интернета, недопустимости ограничения доступа к информации и цензуры, за свободу слова в Интернете и свободу доступа к информации, сохраняли и использовали большие объемы информационных данных обо всех пользователях сети и использовали их в своих политических и экономических интересах. Как отмечает Д. Носетти, «в столь политизированном контексте для США было жизненно важным сохранять контроль над ходом дебатов об управлении Интернетом»[158], и в ходе встречи в Бразилии договориться о существенных изменениях в существующем режиме управления Интернетом не удалось.

В этой ситуации была предпринята очередная попытка легитимировать деятельность ICANN в глазах международного сообщества – а именно создание уже упоминавшийся организации PTI1 октября 2016 года и передача ей функции

---

[155]На конференции в Дубае планировалось усилить государственное регулирование Интернета // IXBT. 6.12.2012. URL: http://www.ixbt.com/news/hard/index.shtml?16/35/25

[156]Зиновьева Е.С. «Цифровой Вестфаль»? [Электронный ресурс] // Эксперты МГИМО. 26.03.2013. URL: /news/experts/document236588.phtml

[157] На конференции NETmundial предложения о темах обсуждения лягут в основу обсуждения вопросов, связанных с управлением Интернетом // NETmundial Официальный сайт. URL: http://netmundial.br/ru/2014/04/07/%D0%BD%D0%B0-%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D0%B8%D0%B8-netmundial-%D0%BF%D1%80%D0%B5%D0%B4%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D1%8F-%D0%BE-%D1%82%D0%B5%D0%BC%D0%B0%D1%85/

[158] Носетти Д. Жизнь после Эдварда Сноудена: будущее управления Интернетом // Коммерсант. 09.04.2014. URL: http://kommersant.ru/doc/2448799

IANA (координации выработки параметров интернет протоколов, управление корневой зоной доменных имен и выделение блоков IP-адресов)[159]. Вместе с тем, подобная реформа не решает проблем с подотчетностью новой структуры и не обеспечивает представительство интересов государств в осуществлении управления интернетом. Хотя создание новой структуры означает прекращение контракта между правительством США и ICANN, указанная организация остается зарегистрированной в США и подчиняется законам этого государства, кроме того, правительства других стран также не получили возможности влиять на принимаемые решения.

«США стремятся закрепить лидерство в глобальном информационном пространстве, сохраняя за собой контроль над ключевыми инфраструктурами Интернета. Вместе с тем, растёт число государств, оспаривающих лидирующие позиции США в режиме управления Интернетом, при этом крупные Интернет-компании, такие как Google и Facebook, воспринимаются как проводники влияния США. Существующая ситуация все чаще трактуется как угроза международной безопасности представителями исследовательского сообщества[160]»[161].

Несмотря на то что Интернет с технической точки зрения работает стабильно, вопрос об управлении Интернетом – это политическая проблема, причем ее значимость возрастает по мере увеличения количества и потенциальной опасности угроз информационной безопасности. «События «Арабской весны», получившие в СМИ название «Twitter-революций», актуализировали проблему информационной безопасности и способствовали стремлению государств укрепить свой суверенитет в глобальном информационном пространстве, что вновь актуализировало проблематику управления интернетом и роль США в этом процессе. Дополнительный импульс придают учащающиеся кибератаки, в частности, атаки вируса Stuxnet на ядерные объекты Ирана в 2011 году, и атаки вируса Wannacry в 2017 году, которые

---

[159] IANA после передачи функций // Официальный сайт ICANN. URL: https://www.icann.org/ru/stewardship-implementation/post-transition-iana-ru

[160] См. напр.: Роговский Е.А. Кибер-Вашингтон: глобальные амбиции. М.: Международные отношения, 2014 и др.

[161] Зиновьева Е.С. «Цифровой Вестфаль»? [Электронный ресурс] // Эксперты МГИМО. 26.03.2013. URL: /news/experts/document236588.phtml

наглядно демонстрируют, что информационные войны и информационное оружие — это уже не абстрактные сценарии футурологов, но вполне реальная международная практика. Передача управления Интернетом на межгосударственный уровень видится как важное условие более безопасного и стабильного Интернета»[162].

«Интернет как глобальная сеть, не знающая границ, вступает сейчас в противоречие с существующей Вестфальской политической системой мира. В информационной сфере мир глобален и взаимозависим, но в политической сфере — разбит на суверенные государства. Значительная часть государств стремится усилить свой контроль над национальными сегментами сети, при этом обеспечив их эффективное участие в общемировых информационных процессах. Подобную цель ставит перед собой и Россия»[163].

Современный режим управления интернетом не отражает изменяющийся международно-политический ландшафт глобального информационного пространства, что в свою очередь порождает угрозы конфликтов и нестабильности. Когда политические решения классифицируются как техническое регулирование, становится возможным их принятие за закрытыми дверями, вне общественного контроля, как это показали разоблачения Э. Сноудена, в результате нарушаются не только демократические процедуры, но и разрушается атмосфера доверия, без которой невозможно сотрудничество. Представляется важным, чтобы политические, экономические и технические вопросы, имеющие отношение к управлению Интернетом, решались при участии всех заинтересованных сторон, так как обеспечить информационную безопасность и сохранить связность Интернета как глобальной системы ни одно государство не в состоянии без многостороннего сотрудничества.

Интернет и вопросы управления Интернетом играют ключевую роль с позиции международной информационной безопасности, так как глобальная сеть становится важным инструментом «проекции» власти государств на

[162]Там же.
[163]Там же.

международной арене: «мягкой силы» при помощи культурного и лингвистического влияния, жесткой силы благодаря кибератакам, кибер-шпионажу и сбору разведывательных данных, а также коммерческой выгоды, благодаря созданию Интернет-бизнеса, а также создавая возможности наиболее влиятельным акторам задавать «правила сети» и параметры, на основании которой использование и управление Интернетом будет осуществляться.

1.3. Политико-экономические аспекты глобальной информатизации

1.3.1. Влияние информационной революции на мировую экономику: политические аспекты

Развитие глобального информационного общества, и, следовательно, проблематика информационной безопасности имеет политико-экономическое измерение. Природа и характеристики глобального информационного пространства во многом определяются деятельностью частного бизнеса, более того, государства при принятии политических решений в сфере безопасности вынуждены учитывать экономические последствия, так как мировая экономика, так же как и экономики национальных государств во все большей степени зависят от Интернета и информационно-коммуникационной среды.

Одним из наиболее значимых последствий развития ИКТ стала трансформация мировой экономики, ключевым компонентом которой становятся отрасли, основанные на информации и коммуникациях. Для описания этого нового явления появляются новые термины «информационная экономика» (синонимом является «цифровая экономика»), содержание которых, однако, является предметом дискуссий. Согласно наиболее общему подходу, ключевой характеристикой информационной экономикой является производство информационных товаров и услуг как источник богатства и создания новых

рабочих мест[164].Как отмечается в докладе ОЭСР, сегодня ИКТ и Интернет настолько плотно вплетены в экономическую активность, что вычленить собственно информационный сектор в мировой экономике и экономике отдельных государств и оценить его представляется довольно проблематичным[165]. ЮНКТАД в рамках более узкого подхода рассматривает электронную коммерцию как основу «информационной экономики», при этом электронная коммерция понимается весьма широко как «покупку и продажу товаров и услуг при помощи электронных сетей», причем сами товары и услуги могут предоставляется как в электронной форме, так и в физической[166].

Формирование информационной экономики не предполагает снижение значимости промышленных отраслей. Если в 1990 гг. ИКТ рассматривались как источник глубинных трансформаций в экономики, то на сегодняшний день они выступают в качестве базовой инфраструктуры, без которой невозможно развитие других высокотехнологичных отраслей. За счет развития информационного сектора рынок становится значительно более масштабным и конкурентным.

Однако проблема «цифрового разрыва» препятствует реализации экономического потенциала ИКТ в глобальном масштабе. «Цифровой разрыв» усугубляет иные виды неравенства – экономическое, социальное, культурное, как на глобальном, так и на внутригосударственном уровнях.

Внимание России к вопросам развития цифровой экономики отражается в ряде документов, принятых в последние годы. В частности, 28 июля 2017 года была утверждена программа «Цифровая экономика»[167]. Программа направлена на создание и развитие инфраструктурных и институциональных условий для развития высокотехнологичного бизнеса, причем в число основных технологий,

---

[164]Cogburn D., Adeya C. Globalization and the Information Economy: Challenges and Opportunities for Africa // UNCTAD African Development Forum '99. Working paper. Addis-Abeba, 1999.P. v. URL: http://archive.unu.edu/africa/papers/cogburn-adeya.pdf

[165] OECD (2012), OECD Internet Economy Outlook 2012, OECD Publishing, Paris. URL: http://www.oecd.org/sti/ieconomy/oecd-internet-economy-outlook-2012-9789264086463-en.htm

[166] Information Economy Report 2015 - Unlocking the Potential of E-commerce for Developing Countries. UNCTAD/IER/2015 UNCTAD, 2015. URL: http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1146

[167] Программа «Цифровая экономика Российской Федерации». Утв. распоряжением Правительства Российской Федерации № 162-р. 28.07.2017. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

задающих рубежи будущего развития отнесены: «большие данные, нейротехнологии и искусственный интеллект; системы распределенного реестра; квантовые технологии; новые производственные технологии; промышленный интернет; компоненты робототехники и сенсорика; технологии беспроводной связи; технологии виртуальной и дополненной реальностей»[168]. В программе отмечается значимая роль, которую играют бизнес-структуры в реализации экономического потенциала инновационного развития страны, основанного на возможностях, предлагаемых информационными технологиями.

Компании используют Интернет и другие ИКТ для повышения производительности и усиления координации обширной сети филиалов, повышения эффективности управления. Как отмечает российский исследователь Е.А. Роговский «компьютеры и информационные технологии увеличили доступ бизнеса к информации, что сделало бессмысленной дорогостоящую вертикальную интеграцию компаний, сократило время и стоимость заключения сделок, сделало более привлекательным коммерческое и технологическое сотрудничество (аутсорсинг)»[169]. Широкое распространение получает также электронная коммерция, причем именно проблема информационной безопасности и доверия пользователей сдерживает потенциал ее развития[170].

Целый ряд вопросов, связанных с экономическими аспектами использования Интернета также имеет важное международно-политическое значение. Среди них такие вопросы, как сетевая нейтральность или количество провайдеров, предоставляющих доступ к сети Интернет.

Экономические вопросы количества провайдеров и конфигурации Интернет-инфраструктуры также имеют значимые последствия с точки зрения информационной безопасности. В частности, незначительное количество Интернет-провайдеров позволило правительству Египта отключить доступ к Интернету в ходе массовых протестов Арабской весны. Вместе с тем,

---

[168] Там же.

[169] Роговский Е.А. США – информационное общество: экономика и политика. М.: Международные отношения, 2008. С. 132.

[170] E-commerce: impacts and policy challenges. // OECD Economic Outlook 67. OECD, 2000. URL: http://www.oecd.org/eco/outlook/2087433.pdf

значительные экономические издержки подобного решения (порядка 90 млн. долларов в сутки) побудило правительство вскоре отказаться от подобной политической меры[171].

Проблематика сетевой нейтральности, приобретающая все более заметное освещение в СМИ, а также заметное место на международной повестке дня, имеет важное политическое измерение (в 2015 году в США был законодательно закреплен принцип сетевого нейтралитета, США также выступает за его внедрение в международную практику). Согласно принципу сетевой нейтральности сеть нейтральна по своей природе и предназначена для передачи информации, вне зависимости от характеристик. Данный принцип и его поддержка на политическом и международно-политическом уровне изначально имели в своей основе экономическую природу – подобный подход ставил компании Интернет-индустрии в более выигрышное положение по сравнению с телекоммуникационными компаниями, обладающими правом собственности на инфраструктуру, и желавшими взимать большую плату за более «тяжелый» трафик, например, за видео и голосовую информацию. Вместе с тем с политической точки зрения реализация подобного принципа предполагает угрозу признания нейтралитета технологий по отношению к политическим последствиям их использования, в том числе с целью нарушения информационной безопасности, как на национальном, так и на международном уровнях.

Широкое распространение в банковском секторе информационно-коммуникационных технологий стимулировало свободу передвижения мировых финансовых потоков. Наибольшее значение имеет развитие Интернет-банкинга и электронных денег. Предоставление банковских услуг в режиме онлайн, или Интернет-банкинг, существует уже достаточно долго. При этом именно информационная инфраструктура финансового сектора является наиболее частым объектом атак, как со стороны преступников, так и в рамках межгосударственного противостояния. И именно эта отрасль рядом авторов

[171] The economic impact of shutting down Internet and mobile phone services in Egypt // OECD official site. 4.02.2011. URL: http://www.oecd.org/sti/ieconomy/theeconomicimpactofshuttingdownInternetandmobilephoneservicesinegypt.htm

рассматривается как перспективная сфера для международного сотрудничества, которое может рассматриваться как первый шаг на пути формирования всеобъемлющего международного режима информационной безопасности[172].

Относительным нововведением являются т.н. электронные деньги. Электронные деньги хранятся и обращаются в электронном виде[173]. Весьма вероятно, что электронные деньги станут глобальным явлением, а это даст повод рассматривать вопрос на международном уровне, дополнив международную повестку дня в сфере информационной безопасности.

Серьезные международно-политические противоречия порождает также широкое распространение криптовалют (Bitcoin и др.), так как контролировать их распространение и использование достаточно сложно[174], что порождает угрозы финансовой безопасности. При этом сама технология блокчейн, лежащая в основе криптовалют рассматривается как эффективная. В целом, информационная безопасность финансовой сферы на сегодняшний день является одним из наиболее острых вопросов международной информационной безопасности.

Таким образом, национальная и международная безопасность в цифровую эпоху тесно связана с экономической проблематикой. Экономическое развитие государства и мировой экономики в целом в современных условиях опирается на информационную инфраструктуру, которая, как отмечают экономисты, наряду с новыми возможностями в сфере транспорта, сделала возможными процессы экономической глобализации[175]. Следует также отметить, что, по оценкам экспертов, большинство атак на информационные ресурсы государств имеют под собой экономическую подоплеку[176].

---

[172]См. напр.: Hyslop M. Critical information infrastructures: Resilience and protection. – Springer Science & Business Media, 2007.

[173] Курбалиа Й. Управление Интернетом / пер. с англ. М.: Координационный центр национального домена сети Интернет, 2010. – С. 120.

[174] Россия объявила bitcoin вне закона // Вести Финанс. 09.02.2014. URL: http://www.vestifinance.ru/articles/39178

[175] См. напр.: Henderson J. Global production networks and the analysis of economic development / Henderson J. , Dicken P., Hess M., Coe N., Yeung H. //Review of international political economy. 2002. №. 3. С. 436-464.

[176]См. напр.: Lezner R. The Cyberwarfare Arms Race By Iran, China And Russia Is Threatening American Finance And Industry // Forbes, 4.07.2014. URL: http://www.forbes.com/sites/robertlenzner/2014/07/04/the-cyberwarfare-arms-race-by-iran-china-and-russia-is-threatening-american-finance-and-industry/

С позиций безопасности, помимо растущей экономической зависимости от ИКТ, а, следовательно, уязвимости государств, значимая роль бизнеса в информационном пространстве может создавать дополнительные угрозы. Информационная инфраструктура бизнеса, находящаяся в частной собственности, становится объектом информационных атак, причем некоторые из них по своим последствиям сопоставимы с угрозами национальной безопасности (в частности, подобный подход отражен в официальных документах Российской Федерации)[177]. Бизнес заинтересован, прежде всего, в собственной безопасности, что препятствует коллективным действиям в данной области. Более того, у частного бизнеса (особенно, это верно в отношении финансовых структур) есть заинтересованность в сокрытии успешных компьютерных атак, что было одной из причин того, что широкая общественность долгое время не осознавала масштаб угроз, связанных с развитием информационного пространства. Как отмечается в отчете компании МакАфи, «Общественность (и зачастую частный сектор) лишь в незначительной степени осведомлены о масштабе угроз вследствие незначительного числа добровольного предоставления информации жертвами кибератак»[178].

Таким образом, бизнес-структуры (в особенности представители финансового и ИТ сектора) выступают в роли влиятельных игроков в сфере информационной безопасности, прежде всего, в ее технологическом измерении. С позиций теории секьюритизации, бизнес-структуры выступают в роли функциональных акторов в обеспечении международной информационной безопасности, имея возможность оказывать влияние на динамику развития секьюритизируемой области. В этой связи международное сотрудничество по обеспечению информационной безопасности, также как и выработка

---

[177] См. напр.: Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Утв. Президентом 3.02.2012. Пр. № 803. URL: http://www.scrf.gov.ru/documents/6/113.html

[178] Alperovitch D. Revealed: Operation Shady RAT // McAfee white paper, 2011. # 3. URL: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

внешнеполитической стратегии России в данной области, будут более эффективны при привлечении заинтересованных влиятельных бизнес-структур.

Во многих странах государства без сотрудничества с бизнесом неспособны предоставить растущее количество общественных благ, в которых нуждается современное общество. Тенденция к государственно-частному партнерству возрастает в таких областях, как образование, здравоохранение и транспорт, и включает вопросы обеспечения национальной безопасности. Исследователями этот процесс рассматривается как слияние военной и гражданской сферы или же как милитаризация гражданской сферы. Не менее значима эта тенденция и в сфере ИКТ[179]. Во многих развитых странах, значительная часть критической информационной инфраструктуры находится в собственности бизнеса. Так, военными всегда использовалась телекоммуникационная инфраструктура, но на современном этапе большая часть военной информации передается через гражданские сети и зависит от их работы. Компьютерные сети стали частью военного потенциала государств, но они также являются основным каналом для распространения мягкой силы[180].

Развитие информационного общества оказывает существенное влияние на мировую экономику, не только усиливая взаимозависимость, но и порождая новые формы экономической деятельности, реализуемые исключительно в онлайн среде. «Интернетизация» мировой экономики имеет политическое значение, в частности, она создает новые вызовы международной информационной безопасности. В целом, именно недостаточно высокий уровень международного сотрудничества по обеспечению информационной безопасности тормозит развитие электронного бизнеса, коммерции и банковского сектора. Однако политически наиболее значимым явлением Интернет-экономики последних лет стало широкое распространение социальных сетей и блогов и иных новых медиа, которые, будучи коммерческими по свой природе, тем не менее, косвенно порождают новые угрозы национальной и международной

[179]International relations and security in the digital age / Ed. by J. Eriksson, G. Giakomello. London, NY: Routlege, 2007. P. 16.
[180] Там же.

безопасности, что ярко проявилось в ходе событий «Арабской весны», получивших в прессе названия «Twitter- » или «Facebook революций».

В этих условиях обеспечение информационной безопасности, как на уровне отдельных государств, так и на уровне международного сообщества, будет более эффективным в случае привлечения бизнеса.

Информационная экономика взаимозависима, что создает новые области совпадения интересов, таким образом, способствуя развитию международного сотрудничества, одной их таких областей может стать защита информационной инфраструктуры финансовых институтов на международном уровне. При этом взаимозависимость в информационной сфере, как уже было показано ранее, не снимает проблему международной конкуренции и конфликтности. В этих условиях развитие технологической и производственной базы в области ИКТ является важнейшим условием обеспечения информационной безопасности государства. При этом роль бизнес-структур в обеспечении информационной безопасности возрастает, вследствие чего государства, заинтересованные в обеспечении экономического роста и развития, вынуждены учитывать интересы бизнеса. В то же время, бизнес-структуры, работающие в сфере ИКТ в развитых и развивающихся странах, в выработке стратегий развития также все чаще ориентируются на государственные интересы в сфере информационной безопасности.

1.3.2. Интернет-компании как акторы мировой политики

Деятельность Интернет-компаний (или компаний «Интернет-индустрии) представляет собой самостоятельную проблему, так как их деятельность в контексте формирования глобального информационного общества обладает рядом отличительных характеристик и порождает специфические международно-политические проблемы. Интернет-компании определяют лицо современного информационного общества, вследствие чего их деятельность имеет значимое

политическое измерение и порождает противоречия на международном уровне. Под компаниями «Интернет-индустрии»[181] (также используется термин «Интернет-компании») понимаются бизнес-структуры, получающие основной доход (более 50% дохода) от предоставления услуг в он-лайн режиме[182].

Политическое значение коммерческой деятельности в данной области весьма велико - Интернет-компании определяют, каким образом пользователи ищут информацию, упорядочивают ее, общаются, формируют контекст, в котором действует пользователь Интернета, управляют его предпочтениями. Наиболее крупными Интернет-компаниями мира, по оценкам аналитиков Boston Consulting Group, являются Amazon, Apple, Facebook, Google, Baidu, Tencent (страна базирования первых четырех – США, последних двух – Китай; причем последние четыре компании являются производителями контента, информационного содержимого Интернета)[183]. В современной цифровой экономике доминирует так называемая олигополия GAFA (Google—Apple—Facebook—Amazon).

Вместе с тем, цифровые компании Китая все более активно выходят на международную арену. Что касается Российской Федерации, наиболее влиятельными Интернет-компаниями на 2017 г. были Яндекс и Mail Group[184]. На российском рынке значительные позиции занимают такие транснациональные Интернет-компании, как Facebook, хотя число пользователей несопоставимо с национальными Интернет-компаниями[185].

В своём прогнозе на 2016 год аналитики Boston Consulting Group оценили общий объем общемировой Интернет экономики в 4.2 триллиона долларов США,

---

[181]Термин «индустрия» в современной экономической науке не обязательно предполагает промышленное производство. Под индустрией понимается «отрасль экономики, в котором фирмы используют аналогичные затраты производственных факторов для создания группы родственных товаров». Экономика: толковый словарь / под общ.ред. И.М.Осадчей. М.: "ИНФРА-М", "Весь Мир", 2000.).

[182]30 российских Интернет-компаний: рейтинг Forbes. // Forbes Russia.27.02.2012. URL:http://www.forbes.ru/tehno/rating-slideshow/79474-30

[183] Dean D. The Connected World. The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy / D. Dean, S. DiGrande, D. Field, P. Zwillenberg // BCG Perspectives. 27.01.2012. URL:https://www.bcgperspectives.com/content/articles/growth_innovation_connected_world_digital_manifesto/

[184]20 самых дорогих компаний рунета – 2017 // Forbes Russia. 27.02.2017. URL: http://www.forbes.ru/kompanii-photogallery/339445-20-samyh-dorogih-kompaniy-runeta-2017

[185]См. напр. Zinovieva E. Can Facebook win a bigger share of the Russian social media pie? // Russia Direct. 4.02.2014. URL: http://www.russia-direct.org/content/can-facebook-win-bigger-share-russian-social-media-pie

что превосходит объем ВВП Германии.[186] Как отмечают специалисты, капитализация Интернет пространства является важным элементом его дальнейшего развития, так как с одной стороны стимулирует развитие технологий, с другой формирует принципы взаимодействия его акторов.[187]

Перечисленные выше компании существуют в рамках конкурентной рыночной среды, которая в совокупности отражается на многих характеристиках глобального информационного пространства. Компании, оперирующие на глобальном Интернет рынке, конкурируют, что обуславливает их заинтересованность в политической поддержке со стороны государств базирования, а политизация информационного пространства предопределяет их готовность участвовать в мировой политике, когда того требуют коммерческие интересы. Следует отметить, что компании, ориентированные на глобальные рынки (и конкурентоспособные), как правило, поддерживают идеи информационной открытости, в то время как компании, ориентированные на внутренние рынки, более склонны выступать в поддержку идей «цифрового суверенитета» и информационной регионализации, формирования относительно обособленных информационных пространств внутри регионов.

Развитие Интернет-компаний, приобретающих все большее влияние, подрывает сложившийся на телекоммуникационном рынке баланс сил, а также возможность правительств контролировать потоки информации, пересекающие границы. С позиций теории политической коммуникации они выступают в роли т.н. «новых привратников», определяющих информационную повестку дня пользователей Интернета, получая, таким образом, значительное политическое влияние[188]. Управление тем, какие точки зрения доносятся при помощи СМИ, может либо использоваться с целью интеграции общества, распространяя взгляды, которые способствуют укреплению единства, или же усиливать

[186] Dean D. The internet economy in the G-20: The $4.2 trillion growth opportunity //White paper, Boston Consulting Group, 2012.
[187]The political economies of media: The transformation of the global media industries. // ed. by Winseck D. Bloomsbury Publishing, 2011.
[188] Ristow B. The New Gatekeepers: Controlling Information in the Internet Age. A report to the Center for International Media Assistance // Center for International Media Assistance. 2013. URL: http://apo.org.au/files/Resource/CIMA_TheNewGatekeepers_May2013.pdf

существующие культурные различия в обществе. До эпохи Интернета, компании, управляемые или контролируемые правительствами, обладающие монополией на телевизионном рынке, выступали против рыночного регулирования данной отрасли или распространения кабельного телевидения.

На протяжении XX века существовал международный консенсус относительно того, что радиопередачи следует осуществлять в границах государств, контрольные и регулирующие функции осуществлял Международный союз электросвязи, который распределял между странами частоты радиовещания. В промежутке между мировыми войнами, существовали двусторонние и многосторонние договоренности (в том числе в рамках Лиги Наций), согласно которым ограничивалась пропаганда, которая могла подорвать устои государственного устройства[189]. С развитием Интернета ситуация изменилась, Интернет не локализован внутри государственных границ и представляет собой глобальную распределенную сеть, что осложняет контроль контента, распространяемого Интернет-компаниями.

Бренд-менеджмент большинства западных Интернет-компаний основан на идеях свободы доступа и распространения информации. Так, компания Google определяет свою миссию как «организация мировой информации, обеспечение её доступности и пользы для всех»[190]. Официальная позиция США заключается в том, что такие компании обеспечивают свободу слова и самовыражения, для незападных государств они выступают в роли инструментов информационного влияния, навязывания западных ценностей. Одна из недавних тенденций в развитии Интернета, связанная, в том числе и с деятельностью крупных Интернет-компаний, связана с появлением т.н. «больших данных». Существенно возрастает политическая роль и влияние Интернет-бизнеса, собирающего «большие данные» о предпочтениях и моделях поведения поисковых систем и социальных сетей, анализ этих данных и использование полученных результатов (по сути персональной информации о предпочтениях пользователей, в том числе в

[189]Price M. Price M. E. The market for loyalties: Electronic media and the global competition for allegiances // Yale Law Journal. 1994. P. 667-705.
[190] About Google: google official site. URL:http://www.google.com/about/company/

сфере политического) открывает новые возможности для информационного влияния, воздействия на индивидуальное и общественное создание.

Можно согласиться с М. Кастельсом в том, что распространение сетей и создание Web 2.0 предлагают уникальную возможность для бизнеса – превращение свободы в услугу, предоставление доступа к глобальным информационным сетям в обмен на получение персональной информации,[191]. Компании Интернет-индустрии активно сотрудничают государствами, особенно сильное (но не абсолютное) влияние на них оказывают правительства стран базирования.

На современном этапе управление информацией, доступной пользователям, становится крайне политизированной темой. В свете событий «арабской весны», получивших в прессе также названия «Twitter-революции» или «Facebook-революции», все больше государств склонны видеть угрозу для национальной безопасности в деятельности Интернет-бизнеса. Интернет-компании рассматриваются как проводники влияния США, подтверждением чему стали дискуссии в ходе конференции в Дубае в декабре 2012 г[192].

Закрытие доступа к социальным сетевым сервисам, управляемым Интернет-компаниями, базирующимся в США, является широко распространенной практикой. Аббревиатура SICK (Syria, Iran, China, North Korea) появилась в Интернете в 2012 году и включает в себя названия стран, в которых запрещен доступ к популярной во всем мире социальной сети Facebook.

«Интернет-компании обладают существенным влиянием, с которым вынуждены считаться государства. Как отмечает Д. Най, Интернет-комании имеют возможность формирования базовых предпочтений акторов мировой политики. Решение о создании определенного программного кода, лежащего в основе продуктов и услуг, принимается компаниями без учета мнения

---

[191] Castells M. Communication, Power and Counter-power in the Network Society // International Journal of Communication. – 2007. № 1.P. 238-266.

[192]Klimburg A. The Internet Yalta: Commentary // Center for New American Security. 5.02.2013. URL:http://www.cnas.org/theinternetyalta

пользователей[193]. М. Кастельс полагает, что компании Интернет-индустрии определяют содержание и формат онлайн-взаимодействий в соответствии с поставленными целями: получение прибыли, приращение «мягкой» или «жесткой» силы, формирование культурных ценностей или все вышеперечисленное. Транснациональные компании Интернет-индустрии обладают возможностями организовывать и управлять сетями массовой коммуникации. Таким образом, в терминологии М. Кастельса, они обладают властью формирования сетей. Формирование сетей – это в большей степени вопрос формата, а не контента. Интернет-бизнес приносит прибыль только в том случае, когда создаваемые форматы коммуникации привлекательны для пользователей, что предполагает интерактивность и свободу выражения. При этом пользователи не придают значения тому, каким образом организован и управляется Интернет, социальные сети и пр.»[194]

По мнению французского аналитика, Д. Носетти, роль этих частных предпринимателей напоминает роль, которую в Европе XVII и XVIII веков играли ост-индские компании: они то объединялись, то соперничали с европейскими государствами, а иногда и полностью игнорировали законодательство последних[195]. Схожей точки зрения придерживается профессор университета в Аархусе В. Кляйнвахтер, который полагает, что в отношении международного регулирования глобальной информационной сферы складывается новая модель международного взаимодействия между государствами, организациями гражданского общества, бизнес-структуры и экспертное сообщество[196].

Исследователи марксистского толка полагают, что характер протекания информационной революции отражает интересы крупных корпораций, которые не только оказывают влияние на рынок и предпочтения пользователей, но и

---

[193] Nye J. Cyberpower. // Belfer center for science in international affairs, 2010. URL:http://www.dtic.mil/dtic/tr/fulltext/u2/a522626.pdf

[194]Зиновьева Е.С. Воздействие компаний интернет-индустрии на мировую политику // Вестник МГИМО Университета. 2013. № 1. С. 44.

[195] Носетти Ж. Жизнь после Эдварда Сноудена: будущее управления Интернетом // Коммерсант . 09.04.2014. URL: http://kommersant.ru/doc/2448799

[196] Kleinwaghter W. Internet co-governance: towards a multilayer multiplayer mechanism of consultation, coordination and cooperation // E-learning and digital media. 2006. № 3 (3). - P. 473–487.

способствуют формированию техно-оптимистской идеологии информационного общества, при этом государства имеют очень ограниченные возможности влияния на действия Интернет-бизнеса. Профессор Вестминстерского Университета К. Фьюкс считает, что современный этап развития Интернета, основанный на широком распространении социальных сетей, является отражением не интересов пользователей, стремящихся к интерактивному взаимодействию и более активному участию в экономическом и политического развития общества и мира в целом, но крупного бизнеса. По мнению К. Фьюкса, после кризиса «дот.комов» в 2000 г.[197], появилась необходимость выработки новых стратегий аккумуляции капитала для Интернет-экономики. Дискурс «новых социальных медиа» решил эту задачу. Бурный рост социальных медиа как новой модели накопления капитала в рамках цифровой экономики сопровождался формированием новой формы технократической идеологии: новые социальные медиа создают уникальные возможности для включенного политического участия, несут с собой «экономическую демократию», создают возможности для новых форм политической борьбы («Twitter революции»), способствуют демократизации. Подобная идеология была необходима, чтобы инвесторы использовали и поддерживали модель накопления капитала, создаваемую индустрией социальных медиа[198].

Таким образом, деятельность Интернет-бизнеса имеет как политическую, так и экономическую подоплеку и она во все большей степени определяется существующей политической системой мира, основанной на примате национальных государств. Несмотря на то, что инфраструктура глобального информационного пространства (как техническая, так и информационная), по большей части принадлежит частным предприятиям, их деятельность ограничена структурой системы международных отношений. В свою очередь, государства, будучи основными элементами системы международных отношений, ввиду следования национальным интересам или преследуя цели достижения

[197] Fuchs C. Dallas Smythe Reloaded: Critical Media and Communication Studies Today. // The audience of commodity in digital age. / Ed. by McGuigan L., Manzerolle V. New York: Peter Lang, 2013.
[198] Там же.

национальной безопасности, могут осуществлять правовое регулирование взаимодействия акторов глобального информационного пространства. В рамках отдельных государств осуществляется правовое регулирование их деятельности, однако международного режима в данной области пока не было сформировано.

Принимая во внимание экономические, информационные и зачастую политические ресурсы, которыми обладают компании, ведущие бизнес, связанный Интернетом и информацией, маловероятно, что обеспечение информационной безопасности, как на уровне отдельного государства, так и общемировом, достижимо без участия бизнес-структур. Нужно сказать, примеры подобного взаимодействия на национальном уровне достаточно многочисленны, конкретные формы реализации зависят от многих факторов, в том числе уровня развития информационной инфраструктуры, характера собственности на информационные ресурсы, а также политического режима. На международном уровне Международный союз электросвязи уже обладает опытом вовлечения бизнеса в реализацию проектов по обеспечению информационной безопасности, в частности, в рамках сети IMPACT, объединяющей под эгидой МСЭ представителей 142 стран и нескольких крупных игроков отрасли информационной безопасности, в том числе российскую компанию «Лаборатория Касперского».

Выводы по главе:

Анализ развития Интернета и ИКТ может быть вписан в более широкий контекст научно-технологического развития. Технологическая и мирополитическая сферы оказывают друг на друга взаимное влияние и информационная революция, следствием которой стало формирование глобального информационного пространства, не стала исключением.

На современном этапе развитие Интернета и ИКТ отражается на всех сферах жизни общества и государства (в экономике, политике, социокультурной

сфере), трансформируя и саму природу мировой политики. Современный этап информационной революции способствует распространению сетевых форм организации в мировой политике, диффузии власти и усилению негосударственных акторов. В свою очередь природа современной международной политики, в частности, рост конфликтности и тенденция к регионализации[199], оказывает влияние на характеристики глобального информационного пространства.

Мирополитическое взаимодействие и обеспечение безопасности в информационном обществе в значительной степени зависит от характеристик и направлений развития Интернета, который является ключевой инфраструктурой формирующегося глобального информационного пространства.

Следует отметить значимость политико-экономической составляющей современной информационной революции, которая влияет, с одной стороны, на повестку дня в области международной информационной безопасности, которая дополняется такими проблемами, как информационная безопасность бизнеса, причем особое значение имеет безопасность финансовой среды, а с другой стороны – способствует расширению субъектной сферы международного взаимодействия в данной области, так как крупный бизнес имеет существенное, пусть и уступающее государствам, влияние на данную сферу.

Интернет как глобальная сеть вступает на современном этапе в противоречие с Вестфальской политической системой мира. В информационной сфере мир глобален и взаимозависим, но в политической сфере — разбит на суверенные государства. Это обостряет межгосударственные противоречия в отношении управления Интернетом и обеспечении международной информационной безопасности. В международном сообществе существуют противоречивые взгляды на то, каким образом должен быть организован Интернет и какова роль государств и негосударственных акторов в его управлении. США стремятся закрепить лидерство в глобальном информационном

[199]См. напр.: Воскресенский А.Д. Структурирование регионального пространства и его основные акторы. Регионализация и трансрегиональное сотрудничество / А.Д. Воскресенский, Е.В. Колдунова, А.А. Киреева // Мировое комплексное регионоведение / Под ред. А.Д. Воскресенского. М.: Магистр-Инфра-М, 2014. – с. 80-107

пространстве, сохраняя за собой контроль над ключевыми инфраструктурами Интернета. Вместе с тем, растёт число государств, оспаривающих лидирующие позиции США в режиме управления Интернетом (в их числе Россия, Китай, большая часть стран постсоветского пространства, а также целый ряд развивающихся государств), при этом крупные Интернет-компании, такие как Google и Facebook, поддерживающие существующую модель управления интернетом и обеспечения информационной безопасности, воспринимаются как проводники влияния США.

Сложившаяся система управления Интернетом, наряду с растущей значимостью угроз международной информационной безопасности ведет к тому, что значительная часть государств стремится усилить свой контроль над национальными сегментами сети. Наметилось перенесения характерных для мировой политики отношений и институтов в глобальное информационное пространство. “Цифровой Вестфаль” (по аналогии с Вестфальским мирным договором, по итогам которого принцип государственного суверенитета лёг в основу международных отношений в Европе, а затем и во всем мире) предполагает формирование такой тенденции развития международной политики в глобальном информационном обществе, которая основана на уважении суверенитета в информационном пространстве (в широкой трактовке, включая как инфраструктурную составляющую, так и вопросы контента). М.М. Кучерявый определяет информационный суверенитет «как это верховенство и независимость государственной власти при формировании и реализации информационной политики. Верховенство реализуется в национальном сегменте, а независимость – в глобальном информационном пространстве»[200]. обладают определенной свободой действий и влияния, но не подрывают государственный суверенитет в информационном пространстве, так как они не ставят своей задачей политического влияния и зачастую выступают в качестве проводников интересов и политического влияния государств базирования.

[200]Кучерявый М.М. Информационное измерение политики национальной безопасности России в условиях современного глобального мира // Дисс. … ученой степени доктора политических наук. СПб: СПбГУ, 2014. С 10.

Таким образом, утверждение Ганса Моргентау, согласно которому «международная политика, как и любая другая есть борьба за власть» сохраняет свою актуальность и в информационном пространстве[201]. Можно согласиться с выводами Д. Ная, который подчеркивает, что «многие пророки нового информационного мира, как и модернисты до них, зачастую недооценивали, насколько новый мир зависит от традиционного мирового порядка, в котором власть основывается на региональных и глобальных институтах». Причем «классические вопросы политики – кто властвует, на каких основаниях и в чьих интересах, - так же применимы к информационному пространству, как и к географическому»[202].

Регионализация глобального информационного пространства указывает на постепенное ослабление влияния США в глобальной информационной сфере. Тенденция к многополярности, характерная для мировой политики в целом, находит свое отражение в глобальном информационном обществе. В этой ситуации, формирование глобального режима информационной безопасности, так же как и глобального режима управления интернетом, как режима гегемонической стабильности не представляется возможным. Международное сотрудничество по обеспечению безопасности в информационной сфере предполагает согласование позиций между рядом наиболее влиятельных игроков, однако с учетом позиций негосударственных акторов, прежде всего, бизнес-структур и организаций экспертного сообщества, занимающихся вопросами технической координации глобальной сети.

[201] Morgenthau H. Politics among nations: the struggle for peace and power. 1973.
[202] Цит по: Роговский Е.А. США: информационное общество (экономика и политика). М.: Международные отношения, 2008. С 291.

ГЛАВА 2. МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА СОВРЕМЕННОМ ЭТАПЕ

2.1.Международная информационная безопасность: подходы к определению понятия

Одно из негативных последствий бурного развития Интернета и других информационно-коммуникационных технологий - возникновение новых форм международных конфликтов, включая информационные войны, сетевые войны, хакерские атаки и т.п. Как утверждает специальный представитель Президента Российской Федерации по международному сотрудничеству в области информационной безопасности А.В. Крутских, «основная озабоченность в сфере обеспечения международной информационной безопасности связана с возможностью применения информационно-коммуникационных технологий в целях, несовместимых с задачами обеспечения международной стабильности и безопасности»[203]. Все больше стран развивают наступательные информационные потенциалы. Террористические организации и преступные группы также используют средства информационного воздействия, которые обладают существенной разрушительной силой.

Доктрина информационной безопасности России дает следующее определение: «под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»[204]. Согласно позиции, зафиксированной резолюциях ГА ООН по данной тематике, информационная

[203]Крутских А.В. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. 2007. № 1 (5). С. 28-37. URL:http://www.intertrends.ru/thirteen/003.htm

[204]Доктрина информационной безопасности РФ от 5.12.2016. Утверждена указом Президента № 646. URL: http://www.scrf.gov.ru/documents/6/5.html

безопасность рассматривается в контексте т.н. «триады» угроз – террористической, военной и преступной[205].

Информационная безопасность появилась в международно-политической повестке дня и, как следствие, в исследовательском и публицистическом дискурсе после окончания холодной войны. Изначально термин «информационная безопасность» использовался для обозначения проблем безопасности компьютеров и компьютерных сетей. Впоследствии термин приобрел значительно более широкий смысл, выходящий за рамки исключительно технологической сферы и включающий вопросы контроля над информационными потоками, обладающими дестабилизирующим потенциалом в масштабах общества, государства и международной системы.

Нужно отметить, что лидерство в области изучения проблем информационной безопасности принадлежит исследовательскому сообществу США. Особо следует выделить концепцию информационных войн второго поколения, разработанную аналитиками RAND Corporation. В соответствии с данной концепцией, информационные атаки рассматривались как атаки нового типа в рамках стратегического противоборства[206]. При этом военные операции нового типа рассматривались как ориентированные на эпистемологическую сферу противника с целью нарушить процесс принятия решений[207].

В России первые исследования влияния информационной революции на национальную и международную безопасность появились в середине 1990-х гг. и представляли собой осмысление западных наработок. Более того, интерес к этой области был обусловлен еще и тем фактом, что после распада СССР США существенно превосходили Россию в области обычных вооружений, а «концепции информационного воздействия предполагали создание

[205] Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/63/37. 02.12.2008.
[206] Molander R. Strategic information warfare: A new face of war. Rand Corporation, 1996.
[207] Szapranski R. A Theory of Information Warfare; Preparing for 2020. AIR UNIV MAXWELL AFB AL, 1995. URL: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA328193

асимметричных угроз противнику, где информационным технологиям отводилась роль мультипликатора силы при минимальных вложениях»[208].

Для раннего периода изучения проблематики информационной безопасности в отечественном и зарубежном научном и военно-политическом сообществе характерно изолированное рассмотрение разных аспектов (компьютерных, организационно-управленческих, психологических и т.д.) информационной составляющей международной безопасности и военно-политических конфликтов (получивших в американских стратегических документах название «информационная война»). Осознание российским руководством и научным сообществом опасности «электронного Перл-Харбора»[209] для критической инфраструктуры, зависимой от информационно-компьютерных средств и потому уязвимой, выход на первый план ассиметричных угроз со стороны негосударственных акторов, заставили рассматривать технические, политические, организационные, психологические и другие аспекты информационной безопасности в комплексе. Широкий подход к информационной безопасности до сих пор характерен для российских исследований данной области. В современной российской исследовательской литературе, как и в официальных документах, международная информационная безопасность рассматривается в комплексе в контексте так называемой «триады» угроз международной информационной безопасности, определяемой через целеполагание ее субъектов, которая включает в себя террористическую, военную и криминальную угрозы[210].

Многие авторы, как российские, так и зарубежные отмечают, что именно военно-политическое измерение угроз безопасности представляет наибольшую угрозу международной стабильности[211]. Кроме того, российский подход к

---

[208]Болгов Р.В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях // Дисс. … ученой степени кандидата политических наук. СПб: СПбГУ, 2011.

[209]Schwartau W. Information Warfare - Chaos on the Electronic Superhighway. New York: Thunder's Mountain Press, 1994; Федоров А.В. Информационная безопасность в мировом политическом процессе. М.: МГИМО, 2006

[210]См. напр.: Molander R. Strategic Information Warfare: A New Face of War / R. Molander, A. Riddile, P. Wilson. CA: Rand Corporation, 1996.

[211] Neuneck G. Civilian and military cyber threats: shifting identities an attribution. // The Cyber Index. International Security Trends and Realities. UNIDIR, 2013. P. 115 // http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

международной информационной безопасности предполагает рассмотрение как технологических угроз безопасности, так и более широкого спектра информационно-психологических угроз (в другой терминологии социо-гуманитарных[212] или политико-идеологических[213]), связанных с распространением и содержанием контента информационных сетей.

Современная научная литература западных исследователей по безопасности в цифровую эпоху, как правило, посвящена анализу следующих тем - защита критических информационных инфраструктур, информационный войны, информационные операции, преступность и терроризм в сфере ИКТ, революция в военном деле. В основном научная литература по данной проблематике сосредоточена на исследовании отдельных аспектов проблематики, ориентирована на лиц, принимающих решения, и мало занимается разработкой и применением теории.

В настоящее время на международной арене можно выделить два конкурирующих секьюритизирующих дискурса в области информационной безопасности. Эти дискурсы находят отражение в исследовательской литературе по тематике информационной безопасности и связаны с расхождениями в подходах государств к определению угроз в сфере ИКТ, подлежащих урегулированию на международном уровне. В рамках этих дискурсов выделяют два основных вида информационной безопасности: информационно-техническую и информационно-психологическую безопасность. Обеспечение информационно-технической безопасности включает в себя защиту, контроль и соблюдение законности и правопорядка в телекоммуникационной сфере (защита от несанкционированного доступа, хакерских взломов компьютерных сетей и сайтов, логических бомб, компьютерных вирусов и вредоносных программ, несанкционированного использования частот, радиоэлектронных атак и пр.). Обеспечение же информационно-психологической безопасности предполагает

---

[212] См. напр.: Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. М., 2004. URL: http://www.iisi.msu.ru/UserFiles/File/publications/Streltsov.pdf

[213] Черненко Е.В. Холодная война 2.0 // Россия в глобальной политике. 2013. № 1. URL: http://www.globalaffairs.ru/number/Kholodnaya-voina-20-15874

защиту психологического состояния общества и государства от негативного информационного воздействия. Термин «кибербезопасность» в исследовательской литературе и дипломатической риторике предполагает, что на международном уровне регулированию подлежат исключительно технологические аспекты информационной безопасности, в то время как термин «информационная безопасность» предполагает обеспечение не только технической безопасности информационных сетей и систем, но и более широкий спектр вопросов, связанный с информационно-психологической безопасностью или регулированием контента.

Секьюритизирующий дискурс	**Референтные объекты безопасности**
Кибербезопасность	Информационно-технические аспекты международной и национальной безопасности: безопасность информационных сетей и систем (прежде всего, защита критических информационных инфраструктур)
Информационная безопасность	Информационно-технические и информационно-психологические аспекты международной и национальной безопасности: безопасность информационных сетей и систем (прежде всего, защита критических информационных инфраструктур) и обеспечение информационного суверенитета (контроль над трансграничными потоками информации, контентом, в том числе передаваемым по социальным сетевым сервисам и новым медиа)

Как правило, в роли секьюритизирующих акторов, как во внутренней политике, так и на международной арене выступают государства, так как сфера

безопасности довольно закрыта, однако они вынуждены также учитывать интересы влиятельного бизнеса.

Отметим, что терминологические различия имеют под собой политические основания и отражаются в дипломатической практике. В данном исследовании в зависимости от контекста используются оба термина (и кибер безопасность, и информационная безопасность). Вместе с тем, основные угрозы безопасности в цифровую эпоху более широкой плоскости, нежели исключительно технологические, поэтому в данной работе международная информационная безопасность трактуется в рамках широкого подхода.

Россия, согласно анализу официальных документов и выступлений официальных лиц, придерживается широкого подхода к определению информационной безопасности, что включает в себя как информационно-технические, так и политико-идеологические аспекты (что связано с негативным влиянием на общественное мнение в стране). Россия выступает за использование термина «информационная безопасность» в ходе международных переговоров. Схожего подхода придерживается Китай. Страны Запада, особенно США, в дипломатической риторике используют термин «кибербезопасность», что предполагает учет исключительно информационно-технических проблем, прежде всего обеспечение стабильной работы информационных сетей и систем, а также защиту данных.

Отметим, что в последние годы среди западных исследователей появляются представители сдержанного подхода, подчеркивающие значимость политико-идеологической составляющей угроз информационной безопасности. В частности, М. Данн-Кавелти, сотрудник Центра исследований безопасности в Швейцарии полагает, что проблема информационной безопасности несводима исключительно к инфраструктурной составляющей, к кибератакам или кибер-инцидентам[214]. Редакторы сборника «Международные отношения и безопасность в цифровую эпоху» используют термины «информационная война», но «кибер-

[214] Dunn M. Securing the digital age: the challenges of complexity for critical infrastructure protection and IR theory // International relations and security in the digital age/ Ed by Eriksson J., Giacomello G. Routledge, 2007. P. 87

терроризм» и «кибер-преступность», таким образом, признавая значимость политико-идеологического противостояния в межгосударственных отношениях и обеспечении безопасности в условиях информационной революции[215].

Д. Най также отмечает значимость информационного воздействия в обеспечении безопасности в конфликтах. Он полагает, что в современных конфликтах, военные силы и нерегулярные силы, комбатанты и гражданское население, физическое разрушение и информационное воздействие тесно переплетены. Более того, наличие камер в каждом мобильном телефоне и программы для редактирования фото на каждом компьютере, лишь усиливают информационную составляющую современного межгосударственного противостояния[216].

«На экспертном уровне ведется работа по согласованию обоих терминологических подходов. В 2011 г. Институт Восток – Запад, базирующийся в США, и Институт проблем информационной безопасности МГУ разработали и согласовали список 20 базовых терминов в сфере информационной безопасности, которые, по мысли экспертов, могли бы лечь в основу возможной двусторонней договорённости между Россией и США[217]. Список включает в себя три группы терминов, классифицированных тематически: поле действий (киберпространство, кибернетическая инфраструктура, киберсервисы, критически важное киберпространство, критически важная кибернетическая инфраструктура, критически важные киберсервисы), виды угроз (киберпреступление, кибертерроризм, киберконфликт, кибервойна, кибербезопасность), способы действий (боевые действия в киберпространстве, кибератака, киберконтратака, оборона и противодействие в киберпространстве, кибервойна, оборонительные возможности в киберпространстве, наступательные возможности в киберпространстве, использование преимуществ в киберпространстве, средства киберсдерживания). Можно согласиться с российским экспертом А.В. Бедрицким,

[215] Introduction // International relations and security in the digital age/ Ed by Eriksson J., Giacomello G. Routledge, 2007. P.
[216] Nye J. S. The Future of Power. – PublicAffairs, 2011. P. 34.
[217] Rauscher K. F., Yaschenko V. Russia–US Bilateral on Cyber Security: Critical Terminology Foundations //New York, USA: EastWest Institute. 2011.

который полагает, что «перечисление терминов, по которым российские и американские эксперты смогли достичь согласия, явно указывает на справедливость официальной позиции российской стороны, настаивающей на необходимости рассматривать проблемы международной информационной безопасности в разоруженческом аспекте»[218]. Показательно, что выработанная терминология основана на узком подходе и не включает в себя социо-гуманитарную составляющую информационной безопасности, что, возможно, объясняется 2011 годом публикации данной работы, то есть до принятия в России официальных документов, где было закреплено приоритетное внимание к социо-гуманитарному измерению безопасности в цифровой сфере»[219].

Общее в двух вышеперечисленных определениях информационной безопасности – их связь с «информационной революцией», так как главные угрозы безопасности рассматриваются как порожденные или усиленные в результате глобальной информатизации. Авторитетный международник А. Уолферс в 1952 году определил национальную безопасность как отсутствие угроз ключевым ценностям общества[220]. Если современные общества, в особенности развитых стран, становятся все более зависимыми от ИКТ, информационные угрозы можно рассматривать как важнейшие угрозы национальной безопасности. В результате информационного воздействия, национальная безопасность, определяемая как угроза ключевым ценностям общества, может оказаться под угрозой. При этом сегодня информационная и кибер безопасность трактуется именно как угроза военно-политического характера.

Исследования безопасности в цифровую эпоху опираются на теорию международных отношений, и работы тех ее представителей, которые анализируют проблематику международной безопасности. В исследованиях безопасности в рамках теории международных отношений можно выделить два направления – традиционалисты (ярким представителем являются работы Ст.

---

[218] Бедрицкий А.В. Международные договорённости по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. 2012. №4. URL: http://www.riss.ru/images/pdf/journal/2012/4/10_.pdf

[219] Зиновьева Е.С. Вызовы и риски глобального информационного общества // Ежегодник ИМИ. Мировая политика: старые проблемы и новые вызовы. 2015. № 3. С. 119.

[220] Wolfers A. " National Security" as an Ambiguous Symbol //Political Science Quarterly. 1952. С. 482.

Уолта)[221] и сторонники расширительного толкования безопасности (среди представителей данного подхода следует особо отметить работы исследователей Копенгагенской школы)[222].

Традиционалисты изучают информационную безопасность, прежде всего, с точки зрения возросших военных возможностей государств, которые также включают в себя разведку и возможности психологического противоборства. Представители данного направления полагают, что технологические нововведения не меняют сути международной безопасности, в основе которой лежит распределение власти между государствами и дилемма безопасности. Успешные действия государства, направленные на обеспечение национальной безопасности, предполагают наращивание военного потенциала, что в свою очередь воспринимается как угроза другими государствами, снижая общий уровень международной безопасности. Наличие подобной «дилеммы безопасности» в цифровой сфере отмечают многие исследователи[223].

Представители Копенгагенской школы, среди которых можно назвать Б. Бузана, О. Уивера и др. полагают, что безопасность может быть определена различными способами. Копенгагенская школа утверждает, что коннотации безопасности устойчивы (угрозы выживанию, требующие срочных действий), а характер угроз и ключевые объекты безопасности могут меняться[224]. К числу таких новых объектов безопасности относят глобальное информационное пространство, которая выступает в роли референтного объекта безопасности, который уже был политизирован и сейчас находится на этапе секьюритизации. Лишь незначительное число работ сторонников расширительного толкования безопасности затрагивают вопросы информационной безопасности.

---

[221] Walt S. M. The renaissance of security studies //International Studies Quarterly. 1991. С. 211-239.
[222] Buzan B., Wæver O., De Wilde J. Security: a new framework for analysis. – Lynne Rienner Publishers, 1998.
[223] См. напр.: Крутских А.В. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. 2007. № 1 (5). С. 28-37. URL:http://www.intertrends.ru/thirteen/003.htm
Neuneck G. Civilian and military cyberthreats: shifting identities an attribution. // The Cyber Index. International Security Trends and Realities. UNIDIR, 2013.P. 115. URL: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf и др.
[224] Там же.

Исследования по вопросам информационной безопасности и информационных конфликтов отражали международно-политические реалии каждого конкретного периода времени. Несмотря на то, что во многих странах после завершения Холодной войны военные бюджеты сократились по многим направлениям, стоит отметить возрастание затрат на сферу информационной безопасности и противодействию связанным с ней угрозам. Соответствующие стратегии принимаются в странах Северной Америки, Европы, России, Китае и других частях мира. Наметилась гонка кибер-вооружений (по мнению экспертов, гонка кибер-вооружений ведется по таким направлениям как кибер-шпионаж и разработка программного обеспечения, направленного против критических информационных инфраструктур[225]).

На современном этапе в государствах происходит создание новых специальных государственных ведомственных подразделений, которые официально декларируют не только защиту государственных и коммерческих компьютерных сетей и систем, но и возможность проведения атак на информационные объекты недружественных государств. Помимо государств, сегодня субъектами информационного противоборства могут являться негосударственные акторы, при этом исследователи отмечают, что в ситуации распространения сетевых форм организации в Интернете происходит таких новых субъектов информационного противоборства, как «сетевое ополчение», подразделения «сетевых войн», входящие в самоуправляемые частные и неправительственные организации и частные военные компании, действия которых могут иметь свою внутреннюю логику, свою мотивацию и цели[226].

Информационные атаки на критические информационные инфраструктуры на сегодняшний день рассматриваются в качестве наиболее значимой угрозы информационной безопасности в ее технологическом измерении. Внедрение

---

[225] См. напр.: Куликова А. Возможна ли гонка кибер-вооружений между Россией и США? // ПИР-центр, 28.01.2015. URL: http://www.pircenter.org/media/content/files/13/14243529940.pdf; Chumley C. U.S. in cyberweapons race with China, Russia // The Washington Times. 20.02.2013. URL: http://www.washingtontimes.com/news/2013/feb/20/us-cyberweapons-race-china-russia/ и др.

[226] Актуальные военные аспекты обеспечения международной информационной безопасности / Под общ. ред. С.В. Короткова. М.: Генеральный штаб ВС РФ, 2008. С. 22.

вируса Stuxnet в автоматизированную систему управления АЭС в Бушере в 2010 г. показало потенциальную уязвимость информационных систем, в том числе обеспечивающих жизненно важные процессы в государствах. В последние годы участились информационные атаки на критические инфраструктуры государств, как с целью шпионажа, так и диверсий. Постоянно совершенствуется информационное оружие, в том числе вредоносное программное обеспечение, появляются новые виды вирусных атак и пр. Как отмечают эксперты, современные супервирусы настолько сложны, что их создание под силу только высококвалифицированным командам специалистов, для чего необходимы временные и финансовые ресурсы[227].

Трансграничный характер ИКТ, их доступность и анонимность и повсеместный характер использования затрудняют решение проблемы. Кроме того, во многих странах большая часть критически важных информационных ресурсов, сетей и систем находится в частной собственности, что обусловливает необходимость привлечения частного бизнеса в обеспечение их безопасности.

Информационные средства воздействия широко используются как в мирное время, так и в условиях межгосударственных вооруженных конфликтов; кроме того, их берут на вооружения террористические и преступные группировки. Информационные средства воздействия расширяют возможности вооруженных сил в конфликтах, получения стратегических преимуществ, в том числе, доступа к секретной информации в мирное время, а также в целях работы с мировым и внутригосударственным общественным мнением. В широком смысле под информационным оружием понимают средства и методы, применяемые с целью нанесения ущерба информационным ресурсам, процессам и системам государства, негативного информационного воздействия на оборонные, управленческие, политические, социальные, экономические и другие критически важные инфраструктуры государства, а также массированной психологической обработки населения с целью дестабилизации общества и государства. Приведем

[227] Демидов О., Симоненко М. Пожар в киберпространстве // Индекс безопасности. 2013. № 1. URL: http://www.pircenter.org/media/content/files/10/13559127940.pdf

определения, выработанные Шанхайской организацией сотрудничества. «Информационное оружие – информационные технологии, средства и методы, применяемые в целях ведения информационной войны»[228]. «Информационная война – противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам или ресурсам, критически важным и другим структурам, подрыва политической, экономической, социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны»[229].

В условиях всеобщего доступа к информации, широкого распространения Интернета особое значение имеет работа с общественным мнением как внутри страны, так и на международной арене. В этих условиях контроль над информационным пространством выступает как инструмент «мягкой силы», т.е. способности навязывать противнику свои цели посредством воздействия на его систему ценностей, установки, восприятие. Вызовы информационной безопасности, прежде всего, связаны с внутренним суверенитетом государств и ставят под вопрос не только информационные инфраструктуры в их технологическом измерении, но возможность правительств контролировать ход событий, обеспечивать общественную стабильность и безопасность.

Таким образом, в результате глобальной информатизации формируется новая среда безопасности и новые вызовы и угрозы национальной и международной безопасности. Государства стремятся контролировать эту сферу, хотя и в разной степени; интересы государств также разнятся, что затрудняет международное взаимодействие. Вместе с тем, растет список общих, разделяемых всеми государствами вызовов, который мог бы стать основой международных договоренностей. Как отмечает президент Всемирного экономического форума К.

[228]Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2009 г. // Международная информационная безопасность: дипломатия мира: сборник материалов / под ред. С.А. Комова. М., 2009. - С. 242.
[229]Там же.

Шваб, в условиях роста вооруженных негосударственных формирований и на фоне все более усложняющегося геополитического ландшафта перспективы создания общей платформы для сотрудничества в отношении ключевых проблем международной безопасности в цифровую эпоху становится задачей критически важной и при этом требующей больших усилий[230].

2.2. Субъекты и характер угроз международной информационной безопасности

«Международная информационная безопасность трактуется, прежде всего, исходя из характера угроз. Традиционно выделялась «триада угроз» международной информационной безопасности — использование ИКТ в террористических, преступных и военно-политических целях (под военно-политическими целями понимается использование ИКТ в межгосударственных конфликтах). В частности, подобный подход к определению угроз был закреплен в ряде резолюций ГА ООН, посвященных проблематике информационной безопасности[231]»[232].

Таким образом, угрозы информационной безопасности, как правило, определяются через целеполагание субъектов, а именно государств, преступных и террористических групп и обусловлены наличием наступательного информационного потенциала. Российский политолог А.В. Манойло определяет субъектов информационного противоборства исходя из следующих характеристик:

- «наличие у субъекта в информационно-психологическом пространстве собственных интересов;

[230] Шваб К. Четвертая промышленная революция. М.: ЭКСМО, 2017. С. 99.
[231] Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/63/37. 02.12.2008. и др.
[232]Зиновьева Е. Международное сотрудничество по обеспечению информационной безопасности // Право и управление. XXIвек.2014. № 4. С. 45.

- наличие в составе субъекта специальных сил (структур), функционально предназначенных для ведения информационного противоборства или уполномоченных на ведение информационного противоборства;
- обладание и/или разработка информационного оружия, средств его доставки и маскировки;
- под контролем субъекта находится сегмент информационного пространства, в пределах которого он обладает преимущественным правом устанавливать нормы регулирования информационно-психологических отношений (на правах собственности, закрепленных нормами национального и международного законодательства) или государственным суверенитетом ...;
- существование в официальной идеологии положений, допускающих участие субъекта в информационном противоборстве»[233].

А.В. Манойло выделяет шесть групп субъектов международного информационного противоборства: «государства и их союзы и коалиции, международные организации, негосударственные незаконные вооруженные формирования и организации террористической, экстремистской, радикальной политической, радикальной религиозной направленности, транснациональные корпорации, виртуальные социальные сообщества, средства массовой информации и массовой коммуникации, виртуальные коалиции»[234]. Достоинством подхода является его комплексный характер, так как он учитывает и информационно-технические, и информационно-психологические аспекты угроз, однако важно также принимать во внимание различия в потенциале акторов информационного пространства.

Согласно распространенной в исследовательском сообществе точке зрения, государство остается ключевым игроком в этой области, сохраняя (хотя и в измененном виде) свою роль гаранта национальной безопасности, даже в

---

[233] Манойло А.В. Объекты и субъекты информационного противоборства. // Официальный сайт проекта ПСИ-Фактор.
URL: http://psyfactor.org/lib/psywar24.htm
[234] Там же.

киберпространстве[235]. Вместе с тем, ряд исследователей утверждает, что на передний план выходят негосударственные акторы. Информационная революция существенно увеличила роль негосударственных акторов – бизнес-структур, сетевых сообществ и отдельных индивидов, которые в информационном пространстве могут как ставить под вопрос безопасность, так и обеспечивать ее[236]. Однако, как было показано в предыдущей главе, несмотря на то, что в информационном пространстве происходит диффузия власти, государства остаются наиболее влиятельными субъектами глобального информационного пространства, в то время как негосударственные акторы, хотя и могут в отдельных случаях действовать самостоятельно, уступают по потенциалу влияния влиятельным государствам. Подобные оценки субъектной сферы информационного и кибер-пространства дает целый ряд российских и зарубежных исследователей[237].

В данной работе мы будем придерживаться подхода, зафиксированного в документах ООН, выделяя т.н. «триаду» угроз международной информационной безопасности исходя из характеристик их субъектов – государств, террористических организаций и преступных групп.

Остановимся более подробно на использовании ИКТ террористическими и преступными группами. Согласно определению, предложенному исследователями А. Колариком и Л. Занчевски, «кибертерроризм – это преднамеренное, политически мотивированная атака субнациональных группировок или иных злонамеренных агентов и индивидов против информации и компьютерных систем, компьютерных программ и данных, направленная против гражданских целей»[238]. Российские исследователи определяют информационный терроризм как совокупность форм активности экстремистских и террористических организаций

[235] Fountain J. E. Building the virtual state: Information technology and institutional change. – Brookings Institution Press, 2004.
[236] Arquilla J., Ronfeldt D. Networks and netwars: The future of terror, crime, and militancy. Rand Corporation, 2001.380 p. URL: https://www.rand.org/pubs/monograph_reports/MR1382.html
[237]См. напр.: Nye J. The Future of Power in the 21st Century, N.Y.: Public Affairs Press, 2011; Бирюков А.В. Современные международные научно-технологические отношения. М.: РОСНОУ, 2014 и др.
[238]Cyber warfare and cyber terrorism. / Ed by L. Janczewski– IGIGlobal, 2007. – P. xxi

в информационном пространстве[239]. Следует отметить, что термин «информационный терроризм» не является общепринятым и универсальным, например, в документах ООН говорится об использовании ИКТ в террористических целях, тем самым подчеркивается, что речь идет не о каком-то особом виде терроризма, но об использовании новых информационных инструментов террористическими организациями[240].

Отечественные специалисты, сотрудники МВД выделяют три основных направления использования ИКТ в целях террористической деятельности:

1. пропаганда идеологии терроризма через СМИ, сеть Интернет и иные средства массовой коммуникации;
2. совершение террористических атак на информационные системы (кибертерроризм)
3. использование ИКТ для обеспечения террористической деятельности (организация и планирование терактов, сбор финансовых средств, вербовка новых членов и пр.)[241].

Террористические структуры наиболее активно используют ИКТ в целях вербовки новых членов, распространения собственной идеологии, размещения информации о своей деятельности, обмена информацией между ячейками и координации действий, также возможно использование кибер-оружия для совершения деструктивных атак, прежде всего, против критической информационной инфраструктуры. Вместе с тем, ключевой ресурс современного информационного пространства с точки зрения террористических организаций – это пропагандистский потенциал. Как отмечают эксперты, пока не было зафиксировано масштабного использования террористическими структурами вредоносного ПОс целью нарушения работы критических информационных

---

[239] Теория и практика информационного противодействия экстремистской и террористической деятельности: монография. / Судиев И.Ю., Смирова А.А., Кундетов А.И., Федотов В.П. МВД РФ Москва-Вологда: Полиграф-Книга, 2014. С. 15.

[240] См. напр.: Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/63/37. 02.12.2008.

[241] Теория и практика информационного противодействия экстремистской и террористической деятельности: монография. / Судиев И.Ю., Смирова А.А., Кундетов А.И., Федотов В.П. МВД РФ Москва-Вологда: Полиграф-Книга, 2014. С. 22.

инфраструктур[242]. Таким образом, более уместно вести речь об информационном терроризме, а не о кибертерроризме.

С точки зрения использования ИКТ террористическими организациями показателен анализ деятельности ИГИЛ (ДАИШ). Действия данной организации в глобальном информационном пространстве характеризуются стратегией, основанной на использовании новых медиа в целях политической Интернет-коммуникации — распространении через онлайн-ресурсы профессионально смонтированных видеороликов, демонстрации фотографий с места боевых действий, публикации сообщений на разных языках в социальных сетях и блогах и др.

Интернет-медиа используются ИГИЛ (ДАИШ) для расширения числа сторонников, привлечения новых бойцов, устрашения врагов и доказательства того, что им действительно удалось создать исламское государство, основанное на религиозных канонах. В западной прессе Интернет-стратегию ИГИЛ (ДАИШ) иронично обозначают как «онлайн-джихад 3.0». Эта стратегия приносит плоды — число мусульман, поддерживающих ИГИЛ (ДАИШ), растет как на Ближнем Востоке, так и в странах Запада. При этом, самой стратегии информационного воздействия недостаточно, она должна подкрепляться успехами в реальном, оф-лайн мире.

Преимуществом Интернета с точки зрения подобной стратегии является отсутствие традиционных «привратников» (газет и телевидения, которые ранее имели возможность определять новостную повестку дня и характер подачи информации), что позволяет выйти на глобальную аудиторию. Попытки западных стран противостоять ИГИЛ (ДАИШ) в среде социальных медиа пока не представляются столь же успешными.

Как отмечают эксперты, в настоящее время, несмотря на территориальные потери, сокращающиеся человеческие ресурсы и финансовые потери, ИГИЛ (ДАИШ) сохраняет позиции, прежде всего, за счет превосходства в информационной сфере. Информационная гегемония для ИГИЛ (ДАИШ) не

[242]Там же.

менее важна, чем превосходство на поле боя и глобальное информационное пространство зачастую играет не меньшее значение в достижении военно-политических целей, чем традиционные военные действия. Успешность информационной политики ИГИЛ (ДАИШ) подтверждается ее стремительным вхождением и новостную повестку дня и успешной политикой, направленной на то, чтобы занять место Аль-Каиды как лидера в области исламистской идеологии, ее привлекательности для потенциальных сторонников по всему миру[243].

Деятельность ИГИЛ (ДАИШ) в этом контексте демонстрирует уязвимость государств, в том числе, влиятельных по отношению к информационным угрозам, в более широком социо-гуманитарном или информационно-психологическом аспекте.

Что касается преступной деятельности в информационном пространстве, то здесь уместнее говорить о киберпреступности, так как основную угрозу представляют технологические аспекты преступной деятельности. Масштабы киберпреступности иллюстрируют данные компании Нортон, согласно которым доходность киберпреступности превышает доходность от незаконного оборота наркотиков[244]. По словам представителя МВД, в России в 2014 году было зарегистрировано 11 тыс. преступлений в сфере телекоммуникаций и компьютерной информации[245]. Данная проблема актуальна не только для России. В 2012 году в странах ЕС произошло увеличение количества киберпреступлений в этой области на 21,2% по сравнению с предыдущим годом, причем ущерб составил почти 800 млн. евро[246]. ИКТ, которыми пользуются преступные группировки, доступны и эффективны. Информатизация финансовой сфере

---

[243] Clarke C., Winer Ch. The ISIS may be failing, but it's strategic communications legacy is here to stay // War on the Rocks. 17.07.2017. URL: https://warontherocks.com/2017/08/the-islamic-state-may-be-failing-but-its-strategic-communications-legacy-is-here-to-stay/?adbsc=social_20170909_1751431&adbid=906404810513047552&adbpl=tw&adbpr=22545453

[244] Norton cybercrime report 2013. // Symantec official site. URL: http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.pptx

[245] Михайлов А. МВД насчитало тысячи преступлений в информационной сфере. // TheatPost.9.02.2015. URL: https://threatpost.ru/2015/02/09/mvd-naschitalo-tysyachi-prestuplenij-v-it-sfere/#sthash.HbtdKNyQ.dpuf

[246] Там же.

делает применение кибертехнологий против информационных сетей финансовых структур наиболее прибыльной сферой киберпреступлений[247].

Спецификой подобного рода преступной деятельности является ее трансграничный характер, а также сложности в идентификации источника противоправного деяния в условиях анонимности в сети Интернет. Именно эта характерная черта киберпреступности обуславливает необходимость международного сотрудничества с целью предотвращения, расследования и устранения последствий киберпреступлений.

Несмотря на значимость таких угроз, как терроризм и преступность в сфере ИКТ, наибольшую опасность представляет столкновение государств с использованием информационного оружия[248]. Многие страны разрабатывают национальные стратегии по обеспечению безопасности критических информационных инфраструктур, а также ведут работы по созданию как оборонительного, так и наступательного информационного потенциала. Можно утверждать, что в современных условиях наметилась гонка информационных и кибер- вооружений, прежде всего, в таких областях как кибер-шпионаж и распространение вредоносных программ, ориентированных на воздействие на критические информационные инфраструктуры.

При этом сложность и, как следствие, стоимость современных супер-вирусов настолько высока, что, их создание и применение по силу лишь государствам. Вместе с тем, есть и более дешевые виды кибероружия, такие как DDoS атаки, которые являются относительно дешевыми и эффективными, но и они активно используются в межгосударственном противоборстве.

В докладе Группы правительственных экспертов ООН от 2010 г. указано, что глобальное информационное пространство становится ареной

---

[247] Касперский: Киберпреступность стала серьезным бизнесом // Security Lab. 23.09.2008. URL: http://www.securitylab.ru/news/359824.php

[248] Neuneck G. Civilian and military cyber threats: shifting identities an attribution. // The Cyber Index. International Security Trends and Realities. UNIDIR, 2013.P. 115. URL: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

разрушительных действий и что киберугрозы становятся одним из важнейших вызовов XXI века[249].

По оценке Министерства обороны России в настоящее время и в обозримом будущем достижение конечных целей войн и вооруженных конфликтов будет осуществляться не столько уничтожением группировок войск и сил противника, сколько подавлением его систем государственного и военного управления, навигации и связи и воздействием на другие критически важные информационные объекты, от которых зависит устойчивость управления экономикой и вооруженными силами государства. Эти тенденции нашли отражение в ходе военных конфликтов последнего десятилетия, где отчетливо проявилась определяющая роль борьбы в информационной сфере[250]. Размывается грань между войной и миром, а также между комбатантами и нонкомбатантами, поскольку любые сети и подключенные к глобальной сети устройства, от военных инфраструктур до гражданских систем могут быть подвергнуты атаке, что, в свою очередь снижает порок критериев наличия войны и создает новые вызовы сложившейся системе международного гуманитарного права.

На глобальном уровне на сегодняшний день не было выработано общепринятого определения информационной войны и информационного оружия. Это связано с различием интересов и позиций государств в информационной сфере, а также нежеланием связывать себе руки в информационном пространстве. Термин «информационная война» большинстве отечественных работ имеет расширенное толкование (информационная война как форма межгосударственного противоборства) и используется в ином смысле, нежели в американских военно-политических и научных кругах[251]. Западные исследователи более склонны использовать термин «кибер-война», которая ограничивается воздействием на компьютерные системы и не включает

[249] General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/65/201, 30 July 2010.

[250] Бурутин А. Новые вызовы и угрозы безопасности России: войны будущего станут информационными // Актуальные военные аспекты обеспечения информационной безопасности. Сборник статей. / Под ред. С.В. Короткова. М.: ГШ ВС России, 2008. С. 3.

[251] См. напр.: Калиновский О.Н. Информационная война – это война? // Военная мысль, 2001, №1. С. 57-58; Szafranski R. A Theory of Information Warfare: Preparing for 2020 / Airpower Journal, 1995 №1. и др.

психологического измерения. Вместе тем, для ряда западных авторов также характерно широкое толкование данного термина. Так, М. Либицки сотрудник Rand Corporation США выделил семь форм информационной войны:

1) война «управления и контроля»;

2) война данных разведки;

3) электронная война;

4) психологические операции;

5) "хакерская война", атаки на информационные системы при помощи программных средств;

6) информационная экономическая война, подразумевающая контроль над торговыми потоками информации (в данном случае информация рассматривается как товар);

7) кибервойна или противоборство в виртуальной сфере[252].

Как правило, проблематику информационных способов ведения войны рассматривают в контексте революции в военном деле. Российский ученый, д.в.н. В.И. Слипченко полагает, что на смену современному шестому поколению войн придут информационные войны, в рамках которых основной поражающей силой станет информационное оружие[253]. Вероятнее всего, полем боя в новых информационных войнах станет именно киберпространство. Как отмечает президент Всемирного экономического форума К. Шваб, следующим этапом эволюции войны будет ведение военных действий с помощью самоуправляемых систем, в том числе боевых роботов и автоматизированного оружия с применением искусственного интеллекта, то есть на основании развитых и дополненных ИКТ[254].

Российский исследователь Р.В. Болгов, сотрудник СПбГУ выделяет следующие основные характеристики информационной войны.

---

[252] Libicki M. What is Information Warfare? Washington: National Defense University, 1995.
[253] Слипченко В.И. Война будущего: прогностический анализ. URL:http://www.scribd.com/doc/26599/B-Слипченко-Война-будущего-прогностический-анализ
[254] Шваб К. Четвертая промышленная революция. М.: ЭКСМО, 2017. С. 110.

1) «Ведение информационной войны достаточно дёшево. Хотя нужно признать, что сейчас существует тенденция к их подорожанию в связи с ростом спроса на средства их ведения, но по общему уровню капиталовложений в их организацию они пока что относительно дёшевы. В отличие от традиционных военных технологий, информационные технологии не требуют обязательной государственной поддержки.

2) Стираются традиционные различия между общественными и частными интересами, между военными действиями и преступным поведением. Стираются признанные межгосударственные границы.

3) Индустриально развитые государства являются наиболее уязвимыми перед лицом информационных атак. Например, США являются наиболее развитой, но при этом и наиболее уязвимой в информационной сфере страной, поскольку их экономика, политика, дипломатия и другие сферы сильно зависят от информационных технологий и систем, и их разрушение грозит разрушению всей жизнеобеспечивающей инфраструктуры внутренней безопасности. Эти опасения нашли отражение в Национальной стратегии внутренней безопасности».[255]

Вместе с тем, в конце 2000-х гг. некоторые авторы ставили под вопрос возможность классифицировать конфликты в информационной сфере как войну. Американский исследователь Л. Гринберг выделяет три основных квалификационных особенности войны: физическое разрушение материальных объектов, территориальный захват и военный характер цели. Гринберг утверждает, что информационная война не отвечает указанным критериям в достаточной мере и не может быть классифицирована как военные действия между государствами.[256] Подобный подход отражает действительность – информационные технологии зачастую используются в мирное время в рамках межгосударственной конкуренции, однако на современном этапе чаще говорят о «гибридных конфликтах», к которым относят и информационное противоборство.

---

[255] Болгов Р.В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях // Дисс. … ученой степени кандидата политических наук. СПб: СПбГУ, 2011.

[256] Greenberg L.T., Goodman S.E., Soo Hoo K.J. Information Warfare and International Law. Washington: National Defense University Press, 1997.

В отсутствии признанных на международном уровне понятий «информационное оружие», «информационная война», а также критериев идентификации подобных феноменов, исследователи все чаще обращаются к термину «гибридная война» или «многомерная война»[257], при этом в современных конфликтах элементы информационного и кибер-оружия используются все чаще[258]. Так, как отмечает эксперт в области международной безопасности, полковник в отставке А.О. Гилев «современная война многомерна. Она сочетает информационное, военное, финансовое, экономическое и дипломатическое воздействие на противника в реальном времени. Предполагается, что массированное и координированное использование всех невоенных методов может оказаться достаточным, чтобы запугать и ослабить оппонента, сведя применение Вооруженных сил к минимуму. Для успеха необходимо, во-первых, обеспечить как можно более полную международную изоляцию объекта воздействия, а во-вторых, заручиться возможностью оказывать на него давление изнутри»[259]. По заключениям экспертов Министерства обороны России в настоящее время военные конфликты, как правило, порождаются не одиночным фактором, а сложным переплетением различных социально-политических, экономических, национальных, религиозных и иных причин. Так и в обозримом будущем достижение конечных целей войн и вооруженных конфликтов будет осуществляться не только уничтожением группировок войск и сил противника, сколько подавлением его систем государственного и военного управления, навигации и связи, а также воздействием на другие критические информационные инфраструктуры, от которых зависит устойчивость управления экономикой и вооруженными силами государства[260]. Таким образом, информационная

---

[257] Гилев А.О. Многомерная война и новая оборонная стратегия // Россия в глобальной политике. №5. 2014. URL: http://www.globalaffairs.ru/number/Mnogomernaya-voina-i-novaya-oboronnaya-strategiya-17101

[258] Куликова А. Возможна ли гонка кибервооружений между Россией и США? // ПИР Центр 28.01.2015. URL: http://pircenter.org/media/content/files/13/14243529940.pdf

[259] Гилев А.О. Многомерная война и новая оборонная стратегия // Россия в глобальной политике. №5. 2014. - http://www.globalaffairs.ru/number/Mnogomernaya-voina-i-novaya-oboronnaya-strategiya-17101

[260] Бурутин А. Новые вызовы и угрозы безопасности России: войны будущего станут информационными. // Актуальные военные аспекты обеспечения международной информационной безопасности. / Под ред. С.В. Короткова. М.: ГШВС России, 2008. С. 3.

компонента в современных конфликтах является одним из ключевых факторов достижения победы.

В соответствии с Кибер-индексом, подготовленным Институтом ООН по вопросам разоружения (ЮНИДИР) более 47 государств разрабатывают программы использования ИКТ в военных целях, при этом 15 из них обладают возможностью использовать ИКТ-потенциал в наступательных целях[261], что стало ответом на неспособность поддерживать баланс сил в области обычных вооружений и, в особенности, оружия массового поражения. Таким образом, в области информационной безопасности сложилась ситуация, описываемая реалистами как «дилемма безопасности».Как убедительно показал в своей работе сотрудник Rand Corporation Мартин Либицки, традиционные меры сдерживания в информационном пространстве малоэффективны вследствие дешевизны и доступности кибероружия, сложности выявления источника угрозы[262]. Разрушительная же способность кибероружия подтверждается тем фактом, что технологии вторжения и кибершпионажа в программное обеспечения в 2013 году были включены в реестр международного Васенаарского соглашения, охватывающего на сегодняшний день 41 государство[263].

Можно утверждать, что конфликтность в глобальном информационном пространстве нарастает, наметилась гонка информационных и кибер-вооружений. Эта гонка на национальном, международном и союзном уровне будет отражать текущий баланс сил на международной арене. В настоящее время в информационном пространстве, по мнению ряда исследователей, как российских, так и зарубежных, наметилась ситуация баланса сил, среди ключевых игроков отмечают США, Россию, КНР, Великобританию, Францию.

---

[261]The Cyber Index International Security Trends and Realities. UNIDIR, 2013. URL: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

[262]См.: Libicki M. Cyber deterrence and Cyberwar. Santa Monica, CA: RAND Corporation, 2009. URL:http://www.rand.org/pubs/monographs/MG877

[263] Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items // Federal Register. A Daily Journal of US Government. 11.05.2015. URL: https://www.federalregister.gov/documents/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items

Военные теоретики утверждают, что информационное пространство становится «пятым полем боя», наряду с землей, морским и воздушным пространством, космосом[264]. Американский политолог Д. Най выделяет следующие характеристики информационного пространства, значимые для мировой политики: «низкая стоимость, анонимность, асимметрия в уязвимости, что позволяет относительно слабым акторам иметь больше возможностей применять жесткую и мягкую силу в киберпространстве, чем в иных традиционных областях мировой политики»[265].

Информационное противоборство становится частью межгосударственной конкуренции и в мирное время. Как заявил Президент Российской Федерации В.В. Путин, в 2014 году было пресечено порядка 74 миллионов кибератак на официальные сайты российских структур и государственных органов[266]. Конец 2014 года ознаменовался кибер-противостоянием США и КНДР, повлекшим за собой кратковременные отключения КНДР от глобального Интернета, вызванными внешними атаками. Ответственность за перебои в доступе к Интернету в КНДР взяла на себя группа хакеров Anonymus. Данный инцидент, несмотря на некоторую надуманность его предпосылок, иллюстрирует значительный информационный потенциал США и готовность его использовать для защиты своих национальных интересов.

В 2014 году США также наложили эмбарго на предоставление товаров и услуг населению Крыма, под действие которого подпадает и сфера ИКТ. Одним из последствий может стать «Интернет-блокада» Крыма в результате блокировки Gmail, Skype, закрытия доступа к Firefox, Google Chrome или Java. Таким образом, межгосударственные споры переносятся в информационную сферу, а негосударственные акторы, такие как бизнес-структуры и общественные движения, выступают скорее в роли проводников государственных интересов, чем независимых игроков.

---

[264] Lewis J., Timlin K. Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization, UNIDIR, 2011.

[265] Nye J. CyberPower, Belfer Center for Science and International Affairs, 2010.P. 1.

[266] Путин: ФСБ в 2014 году пресекла 74 миллиона кибератак // РИА Новости. 26.03.2015. URL: http://ria.ru/defense_safety/20150326/1054622560.html

Информатизация порождает новые угрозы для государств-лидеров, усиливая асимметричную составляющую современных конфликтов, в результате чего уязвимыми оказываются развитые в технологическом плане государства. Сложившаяся ситуация может быть обозначена как «цифровой парадокс мощи» на международной арене, в рамках которого акторы в рамках глобального информационного пространства становятся не только более влиятельными, но и более уязвимыми; то есть ИКТ, усиливая акторов, прежде всего, государства, делают их же более уязвимыми по отношению к угрозам информационной безопасности.

Военная мощь США в сфере ИКТ и развитие информационного оружия лишь провоцирует глобальную конфликтность, в том числе за счет попыток противников США создать собственные системы информационного оружия или дать ассиметричный ответ США иным способом, в том числе путем развития ядерных программ, и в действительности ослабляет безопасность, для обеспечения которой предназначались[267]. Кроме того, двоякое влияние ИКТ на международную безопасность проявляется, с одной стороны, в их содействии демократизации (что и является их целью в соответствии с официальной позицией США) и, следовательно, снижению конфликтности. С другой стороны, ИКТ являются удобным инструментом для создания асимметричных угроз и наращивания политического влияния, результатом чего становится провоцирование новых вооруженных столкновений[268] и гонка вооружений.

Таким образом, силовое воздействие на информационные ресурсы и системы государств является реальностью сегодняшнего дня, и масштабы его будут только расширяться. Информационное оружие обладает ударной силой в ее традиционном понимании (то есть позволяет физически уничтожить или вывести из строя объекты критически важной инфраструктуры противника), не требует создания специализированных производит и сложных систем эксплуатации и использования. Анализ масштабов существующих программ военного

[267]Болгов Р.В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях (политические аспекты). Автореф. дис... канд. полит.наук. СПб.: СПбГУ, 2010. С. 12.
[268] Там же. С. 13.

использования ИКТ, проведенный Министерством обороны России, который включил в себя исследование содержания проводимых мероприятий, объемы их финансирования и военно-технического обеспечения, показал, что превосходство в информационной сфере рассматривается как один из факторов достижения целей национальной стратегии в специфических условиях информационной революции. Для этого создаются специализированные подразделения в структурах вооруженных сил и специальных служб, разрабатываются концептуальные документы, регламентирующие вопросы подготовки и ведения информационных операций, проводятся соответствующие учения[269].

2.3. Объекты международной информационной безопасности

2.3.1. Основные подходы к определению объектов международной информационной безопасности

Согласно Копенгагенской школе, под секьюритизируемым объектом (т.е. применительно к данному исследованию, объектом международной информационной безопасности) понимается сфера, явление, феномен, который рассматривается в рамках секьюритизирующего дискурса как подвергающийся жизненно важной опасности и обладает легитимный правом на выживание[270]. Как отмечают авторы, для понимания специфики секьюритизации как интерсубъективного феномена, важно также понимание специфики секьюритизуемого объекта, свойства которого в значительной степени определяют характеристики дискурса в сфере безопасности.

Российский эксперт политолог А.В. Федоров выделяет следующие конкретные сферы, которые могут стать объектом информационного воздействия:

[269]Бурутин А. Новые вызовы и угрозы безопасности России: войны будущего станут информационными. // Актуальные военные аспекты обеспечения международной информационной безопасности. / Под ред. С.В. Короткова. М.: ГШВС России, 2008. С. 5.
[270] Buzan B., Wæver O., De Wilde J. Security: a new framework for analysis. Lynne Rienner Publishers, 1998.C. 36.

- органы управления государства и его вооруженные силы;

- информационные управляющие системы гражданской инфраструктуры (телекоммуникационные, включая средства массовой информации, транспортные, энергетического комплекса, финансового и промышленного секторов);

- управляющие элементы военной инфраструктуры (системы связи, разведки, боевого управления, тылового обеспечения, управления оружием);

- линии, каналы связи и передачи данных;

- информация, циркулирующая или хранящаяся в системах управления;

- общество в целом (как гражданское население, так и личный состав вооруженных сил), его государственные, экономические и социальные институты;

- руководящий состав и персонал автоматизированных систем управления, участвующий в процессе принятия решений[271].

Как отмечает А.В. Манойло, объектом информационного противоборства и, как следствие, информационной безопасности является «любой объект, в отношении которого возможно осуществление информационного воздействия (в том числе — применение информационного оружия) либо иного воздействия (силового, политического, экономического и т. д.), результатом которого будет модификация его свойств как информационной системы»[272].

Согласно Доктрине информационной безопасности Российской Федерации, национальные интересы России в области информационной безопасности, имеющие международное измерение включают в себя: защиту информационных ресурсов (в современной терминологии – информационной инфраструктуры), а также возможность управления контентом, пересекающим государственные

[271] Федоров А.В. Информационная безопасность в мировом политическом процессе. М.: МГИМО (У) МИД России, 2006. С. 132.
[272] Манойло А.В. Объекты и субъекты информационного противоборства // Пси фактор, 2003. URL: http://psyfactor.org/lib/psywar24.htm

границы. Таким образом, именно эти сферы являются референтными объектами безопасности, то есть рассматриваются как подвергающиеся экзистенциальной опасности.

Во внешнеполитической риторике и исследовательских трудах по информационной безопасности существуют конкурирующие дискурсы относительно того, что представляет собой референтный объект безопасности – кибербезопасности ограничивается информационно-технической составляющей безопасностью, в то время как информационная безопасность предполагает рассмотрение также широких социо-гуманитарных аспектов безопасности. Отметим, что подобные расхождения в подходах нашли свое отражение в дискуссиях на уровне ООН. В частности, ходе дискуссий о мандате Группы правительственных экспертов ООН по информационной безопасности 2014-2015 гг. споры велись о том, будет ли группа обсуждать лишь вопросы обеспечения безопасности критических инфраструктур (информационно-технологическая составляющая безопасности) или же вопросы контента (социо-гуманитарная составляющая)[273]. В данной работе также будет использована подобная классификация объектов безопасности – информационно-технологическая составляющая (в рамках которой наибольшую актуальность представляют вопросы защиты критических информационных инфраструктур), а также социо-гуманитарная составляющая (в рамках которой сегодня на международной арене наибольшую дискуссию вызывает распространение новых социальных медиа и возможность их использования в политических целях).

Наиболее дискуссионным объектом информационной безопасности является общество. Если общество вошло в информационную стадию своего развития, то обеспечение информационной безопасности для такого общества является противоречием в понятиях. Информационное общество должно по

[273] Developments in the Field of Information and Telecommunications in the Context of International Security. Factsheet. // United Nations Office for Disarmament Affairs. June, 2013. URL: http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf

определению уметь работать с информацией и иметь иммунитет против информационного манипулирования.

2.3.2. Обеспечение безопасности критических информационных инфраструктур

Нарушение работы критических инфраструктур может повлечь за собой серьезные последствия с точки зрения национальной безопасности государства. На сегодняшний день значительная часть значимых с точки зрения национальной безопасности объектов зависит от информационных технологий и систем, вследствие чего актуализируется проблема защиты критически важных информационных инфраструктур. Также выделяют международно-значимые критические информационные инфраструктуры (имеющие ключевое значение для группы стран или всего мирового сообщества), такие как система доменных имен и адресов Интернета, а также глубоководные кабели, обеспечивающие работу транснациональной сети Интернет. Однако ввиду высокой политизированности проблемы международного управления Интернетом понятие международной / глобальной критической информационной инфраструктуры не закреплено в официальных документах государств или международных организаций.

Защита критической информационной инфраструктуры на уровне отдельной страны затрагивает вопросы национальной безопасности и потому входит в компетенцию государства. Тем не менее большая часть инфраструктур находится в собственности частного бизнеса, поэтому государство и бизнес вынуждены совместно нести ответственность за их безопасность и стабильное функционирование.

«Значимость защиты критически важных информационных инфраструктур на современном этапе возрастает по ряду причин, среди которых:

- широкое распространение информационных технологий, в том числе в целях обеспечения эффективной работы большинства инфраструктур и систем государства и бизнеса;

- возрастающая зависимость общества и государства от нормального функционирования критических инфраструктур;

- рост сложности и, следовательно, уязвимости информационной составляющей критической инфраструктуры; сложные информационные системы чувствительные не только в отношении информационных атак, они также подвержены сбоям в работе по причине ошибок в программном обеспечении, неточностей персонала и др.; выявить истинную причину неполадок зачастую бывает непросто»[274].

Попытки выработать общепринятое определения термина «критически важная инфраструктура» на глобальном уровне не увенчались успехом. На сегодняшний уровень государства самостоятельно определяют, что относить к критически важным инфраструктурам. Списки жизненно важных инфраструктур разнятся от страны к стране и определяются в соответствии с со спецификой политического режима, уровнем общественного и экономического развития, степенью информатизации различных отраслей и сфер деятельности, а также иными особенностями государств[275].

Остановимся подробнее на определениях критических инфраструктур США и России, а также определениях, даваемых такими международными организациями, как ШОС и ЕС (прежде всего, ввиду того, что практика защиты критических информационных инфраструктур наиболее развита в США и странах ЕС, в то же время ШОС является одной из площадок на которой России удается успешно продвигать инициативы международного сотрудничества в данной области). Патриотический акт (Patriot Act) США 2001 г. дает следующее определение: «критические инфраструктуры – это системы и ресурсы, физические

[274] Коротков А.В., Зиновьева Е.С. Безопасность критических информационных инфраструктур в международном гуманитарном праве // Вестник МГИМО – Университета. 2011. № 4 С. 155.
[275] International critical information infrastructure protection handbook 2008 / 2009 / ed. by A. Wenger, V. Mauer, M. Cavelty. ETH Zurich: Center for Security Studies, 2009. – 648 p.

или виртуальные, настолько значимые для США, что их разрушение или нарушение нормальной работы способно подорвать военно-политическую безопасность государства, экономическую стабильность, здоровье граждан и общественный порядок или повлечь за собой несколько вышеуказанных факторов в любой комбинации»[276].

Исследователи, сотрудники Института проблем информационной безопасности МГУ, дают следующее определение: «Под инфраструктурой будем понимать набор отдельных взаимосвязанных структурных элементов системы, поддерживающих ее функциональность (работу по назначению). Под критической инфраструктурой будем понимать набор отдельных взаимосвязанных элементов, поддерживающих функциональность национально значимых для России сфер жизнедеятельности. Под критически важной информационной инфраструктурой будем понимать набор отдельных программно-аппаратных, сетевых и информационных компонентов, поддерживающих функциональность национально значимых для Росси сфер жизнедеятельности»[277]. Согласно проекту Федерального закона о безопасности критической информационной инфраструктуры Российской Федерации от 2013 года под критической информационной инфраструктурой понимается совокупность автоматизированных систем управления производственными и технологическими процессами критически важных объектов и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, а также информационных систем и сетей связи, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка[278]. В 2017 году в России был принят закон «О безопасности критической информационной инфраструктуры». В список отраслей, регламентируемых законом вошли «энергетика, транспорт, связь, наука,

[276] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. H.R. 3162.
[277]Критически важные объекты и кибертерроризм. Ч. 1. Системный подход к организации противодействия / О.О. Андреев и др.; под ред. В.А. Васенина. М.: МЦНМО, 2008. С. 37.
[278] Федеральный закон о безопасности критической информационной инфраструктуры Российской Федерации. Проект. URL: regulation.gov.ru/get.php?view_id=3&doc_id=12366

здравоохранение, топливно-энергетический комплекс, банковская и иные финансовые сектора, атомная энергетика, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленность» [279]. В соответствии с законом операторами КИИ могут быть только российские юридические лица.

В Соглашении ШОС по информационной безопасности 2009 г. приводится следующее определение: «Критически важные инфраструктуры – объекты, системы и институты государства, воздействие на которые может иметь последствия, прямо затрагивающие национальную безопасность, включая безопасность личности, общества, государства»[280]. В этом же документе «информационные инфраструктуры – совокупность технических средств и систем формирования, создания, преобразования, передачи, использований и хранения информации».

Терминологическая база, применяемая на уровне ЕС, нашла отражение в Директиве Совета ЕС «О европейских критических инфраструктурах и мерах по их защите». Критическая инфраструктура в этом документе представлена как «средства, системы или их часть, расположенные в странах ЕС, которые имеют важное значение для поддержания жизненно важных общественных функций, здравоохранения, безопасности, обороны, экономического и социального благополучия народа и выход из строя которых или их разрушение повлекут серьезные последствия для стран-членов ЕС в результате сбоя поддержания вышеперечисленных функций»[281].

Подводя итог рассмотрению различных определений, отметим, что главной характеристикой критической инфраструктуры является ее ключевое значение для безопасности общества и государства. Критически важные инфраструктуры

---

[279] Королев И. Защиту критической инфраструктуры от кибератак поручат ФСБ // CNews. 07.07.2017. URL: http://www.cnews.ru/news/top/2017-07-07_zashchitu_kriticheskoj_infrastruktury_ot_kiberatak

[280] Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2009 г. // Международная информационная безопасность: дипломатия мира: сб. материалов / под ред. С.А. Комова. М., 2009. С. 242.

[281] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

могут быть военными и гражданскими объектами, а также иметь двойное назначение. В информационной сфере гражданские и военные объекты тесно переплетены. В таблице 1 соотносится российское и американское видение критических инфраструктур государства.

Таблица 1. Критические информационные инфраструктуры России и США[282].

Критические инфраструктуры		
Российская Федерация[283]	США[284]	Военная / гражданская сферы применения
Здравоохранение	Здоровье общества	Гражданские объекты
-	Службы экстренного реагирования	Гражданские объекты
-	Национальные памятники	Гражданские объекты
Сельское хозяйство	Питание и сельское хозяйство	Объекты двойного назначения
Водоснабжение	Вода	Объекты двойного назначения
Государственное управление	Государственное управление	Объекты двойного назначения
Очень большие информационные системы	-	Объекты двойного назначения
Информационные и телекоммуникационные сети	Информационные и телекоммуникационные сети	Объекты двойного назначения
Энергетика	Энергетика	Объекты двойного назначения

[282] Rauscher K., Korotkov A. Working towards rules for governing cyber conflict. Rendering Geneva and Hague conventions in cyberspace // East-West institute. 2011. URL:http://www.ewi.info/working-towards-rules-governing-cyber-conflict

[283] О безопасности: закон РФ (с изменениями 02.03.2007) от 05.03.1992; Стратегия национальной безопасности России до 2020 г.: указ Президента РФ № 357 от 12.05.2009.

[284]Critical Infrastructure Protection: Executive Order 13010 // Federal Register, July 17, 1996. Vol. 61, No. 138; White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive No.63; Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council // Federal Register, Vol. 66, No. 196. October 8, 2001; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 H.R. 3162; The National Strategy for Homeland Security; U.S. Department of Homeland Security. July 16, 2002; The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets: White House, Executive Office of the President. February 2003; Homeland Security Presidential Directive 7, HSPD-7. December 2003.

Теплоснабжение	-	Объекты двойного назначения
Банковская и финансовая системы	Банковская и финансовая системы	Объекты двойного назначения
Транспортная система	Наземный и водный транспорт	Объекты двойного назначения
	Химическая промышленность и взрывоопасные материалы	Объекты двойного назначения
Индустрия	Критически важное производство	Объекты двойного назначения
-	Почтовая служба	Объекты двойного назначения
Муниципальное управление		Объекты двойного назначения
Гражданская оборона		Объекты двойного назначения
-	Военно-промышленный комплекс	Военная цель
Оборона		Военная цель

На сегодняшний день критические информационные и традиционные инфраструктуры сосуществуют. Однако, в условиях формирования «цифровой экономики» наблюдается все более широкое распространение информационных инфраструктур, т.к. они более экономичны, эффективны, эргономичны. В таблице 2 сопоставляются характеристики традиционных и информационных критически важных инфраструктур.

Таблица 2. Традиционные и информационные критические инфраструктуры[285].

Традиционные критические инфраструктуры	Критические информационные инфраструктуры
- человеческий контроль над функционированием; - человеческого регулирование меж инфраструктурного взаимодействия; - иерархические тенденции в использовании. Примеры: госпитали, в которых ведутся бумажные записи и учет, система контроля полетов, основанная на радиосистемах и др.	- функционирование в режиме реального времени с опорой на программное обеспечение (напр., искусственный интеллект); - сложный и взаимозависимый характер меж инфраструктурного взаимодействия; - использование «снизу – вверх»; - повседневная поддержка исходит от гражданского сектора, особенно в городских районах. Примеры: информационная финансовая система, автоматизированная система контроля полетов и др.

Информационные инфраструктуры более уязвимы по сравнению с традиционными в виду доступности и анонимности, а также значительной разрушительной силы информационного оружия. «Сложность и взаимозависимость информационных систем ведет к тому, что последствия нарушения их нормальной работы могут быть непредсказуемыми, в наихудшем варианте вызвать «эффект домино». Таким образом, именно воздействие на критические информационные инфраструктуры является наиболее опасным для

[285]Там же.

общества и государства, может спровоцировать беспорядки, нестабильность, волнения»[286].

«Современные системы включают в себя элементы традиционной физической инфраструктуры, работа которых обеспечивается программным обеспечением и иными информационными системами и ресурсами. Маршрутизаторы, сетевые кабели уязвимы по отношению к традиционному оружию. Нормальную работу виртуальных элементов, таких как программное обеспечение, стандарты, в большинстве случаев невозможно нарушить с помощью традиционных вооружений, однако их можно разрушить непрямым способом, с помощью информационного оружия, например, вирусов, вредоносного программного обеспечения, «червей», закладок и др.»[287]

Уникальность информационного оружия заключается в том, что, развивая свою гражданскую информационную инфраструктуру, государства создают материальную основу для применения информационных технологий в военных целях. Чем выше научно-технический потенциал государства, тем шире набор потенциальных мишеней информационного противоборства: телекоммуникации и связь, космические аппараты, автоматизированные системы управления войсками и оружием, финансовой, банковской и коммерческой деятельностью, энергосистемы и т.д.[288]

Как показал опыт атак вируса Stuxnet на ядерные объекты Ирана, важнейшей угрозой в рамках информационной войны является воздействие на критические инфраструктуры государства посредством нарушения нормального функционирования информационных сетей и систем, обеспечивающих их работу.

Как доказывает американский исследователь, сотрудник Rand Corporation М. Либицки, традиционные меры сдерживания в информационном пространстве малоэффективны вследствие дешевизны и доступности для террористических и

---

[286] Коротков А.В., Зиновьева Е.С. Безопасность критических информационных инфраструктур в международном гуманитарном праве // Вестник МГИМО – Университета. 2011. № 4 С. 155.
[287] Там же.
[288] Бурутин А. Новые вызовы и угрозы безопасности России: войны будущего станут информационными. // Актуальные военные аспекты обеспечения международной информационной безопасности. / Под ред. С.В. Короткова. М.: ГШВС России, 2008. С. 4.

преступных группировок информационного оружия, сложности выявления источника угрозы[289]. Возрастает актуальность уточнения международно-правовой базы, регулирующей глобальное информационное пространство. Наибольшую опасность представляет возможный асимметричный ответ на использование агрессивного информационного потенциала, в том числе с использованием обычных вооружений.

Как уже было отмечено выше, информационные формы оружия привнесли много нового в формы и методы ведения войны. Ниже представлены характеристики информационного оружия, которое может быть использовано против критических информационных инфраструктур.

Таблица 1. Особенности конвенционального и информационного видов вооружений[290].

Конвенциональное	Информационное
- основано на использовании энергии (электромагнитной, кинетической или ядерной), химических и биологических реакций; - цель – материальная; - инструменты специально разработаны для вооруженного конфликта; - доступ к наиболее опасным образцам ограничен; - даже базовые образцы стоят дорого.	- основано на использовании информации и логики; - цель – контроль или получение информации; - имеют преимущественно гражданское предназначение; - низкая стоимость (продолжает снижаться); Примеры: «черви», «вирусы», удаленный контроль, кража паролей и др.

[289]См. Libicki M. Cyber deterrence and Cyberwar.CA: RAND Corporation, 2009. 238 p. URL:http://www.rand.org/pubs/monographs/MG877.html

[290] Rauscher K., Korotkov A. Working towards rules for governing cyber conflict. Rendering Geneva and Hague conventions in cyberspace // East-West institute. 2011. URL:http://www.ewi.info/working-towards-rules-governing-cyber-conflict

Примеры традиционного вооружения, доработанного с помощью ИКТ: GPS, сетевые подразделения и т.д.	

Действительно, информационное оружие привносит трансформации в характер протекания вооруженных конфликтов. Несмотря на то, что в настоящее время в вооруженных конфликтах информационные, так и традиционные типы вооружений используются совместно, по мере технологического развития и роста зависимости всех жизненно важных систем государства от информационных технологий появляются стимулы для создания все более продвинутых систем информационного оружия, направленных на полное уничтожение, нарушение режима нормальной работы критических информационных инфраструктур, перехват их управлением или же сбор чувствительной информации о их работе. Подобные виды информационного оружия, как показывает практика, могут быть использованы как в военное, так и в мирное время.

«Опираясь на определения информационного оружия и критических инфраструктур, можно выделить четыре принципиально различных направления информационного противоборства:

- использование традиционных вооружений против традиционной критической инфраструктуры (ситуация, аналогичная войнам XX века, подпадает под действие международного гуманитарного права);

- использование традиционных вооружений против сетевой критической инфраструктуры (критической информационной инфраструктуры) – маловероятно;

- использование информационных вооружений против традиционной критической инфраструктуры – атака с использованием глобальной системы позиционирования (GPS, ГЛОНАСС и др.) на транспортные и иные инфраструктурные сети, сетевые войска, атака с видео поддержкой, атака

дистанционно управляемого воздушного аппарата на объекты критической инфраструктуры;

- использование информационных вооружений против сетевой критической инфраструктуры (критической информационной инфраструктуры) – собственно войны будущего; атака с помощью программного обеспечения на правительственные информационные системы, закладки и др.»[291]

Как представляется, именно последний вид информационного противоборства является наиболее опасным и может быть отнесен, согласно приведенной выше классификации В.И. Слипченко, к седьмому поколению войн, войнам будущего. В этих условиях важным фактором обеспечения безопасности критических информационных инфраструктур становится запрещение использования информационного оружия (первоначально, обсуждалась демилитаризация информационного пространства, но в условиях гонки информационных вооружений данная тематика утратила актуальность).

Согласно позиции России важно не допустить международной легитимации использования информационных технологий против критических инфраструктур государства. Достижение данной цели возможно только при условии широкого международного сотрудничества, в том числе направленного на правовое регулирование вопросов информационного противоборства.

2.3.3.Социальные медиа в контексте «цифровой дипломатии» и информационной безопасности

В настоящее время социальные медиа и Web 2.0 технологии являются важной составляющей политического процесса, как в рамках отдельного государства, так и на уровне транснациональной политической среды[292]. Интернет стал платформой для политического участия и политического

[291]Коротков А.В., Зиновьева Е.С. Безопасность критических информационных инфраструктур в международном гуманитарном праве // Вестник МГИМО – Университета. 2011. № 4 С. 155.

[292] О транснациональной политической сфере см. Мельвиль А.Ю. Становление транснациональной политической среды и "волны" демократизации // Современные международные отношения и мировая политика: Учебник для вузов / Отв. ред. А.В. Торкунов; МГИМО(У) МИД России. М.: Просвещение, 2004. С. 106-142.

дискурса[293][294].Можно сказать, что социальные медиа играют значительную роль экстрапарламентарной политической активности, создавая возможности для новых форм политического участия, которые без них были бы невозможными. Наметилось формирование новой подвижной публичной сферы, сетевых объединений граждан на основании горизонтальной гражданской коммуникации, которые усиливаются в информационном пространстве. Исследователи отмечают комплексный характер взаимодействия между Интернетом и динамикой социальных движений, а также основными политическим структурами и современными культурным контекстом, который формирует социальные движения[295].Интернет создает условия для коммуникации в глобальном масштабе, благодаря чему сетевые сообщества могут создаваться без временных и пространственных ограничений[296].В условиях широкого распространения новых медиа границы между политикой, культурными ценностями, формированием идентичностей и коллективной поддержкой становятся размытыми, политика становится не только инструментом для достижения целей, но даже приобретает черты перформанса, перемешанного с формированием идентичности он-лайн.

Выше обозначенные тенденции вступают в противоречие с Вестфальской политической системой мира. Новые медиа, спутниковая связь, глобальная телефония легко пересекают государственные границы и ставят под вопрос способность государства контролировать политические коммуникации. Традиционно государства выступают в качестве источника формирования политических дискурсов, стремятся исключить из информационного пространства дестабилизирующие дискурсы, и при этом усилить национальную идентичность при помощи политической коммуникации. Как отмечал британский

[293] Дискурс – термин, широко используемый в различных дисциплинах и научных школах. Наиболее широко распространено лингвистическое определение, согласно которому дискурс – это вербальная конструкция более высокого уровня, чем предложение. Дискурс анализ – исследование не только языковых конструктов одного говорящего, но взаимодействие между двумя и более субъектами, а также лингвистическими правилами и конвенциями, которые используются и управляют дискурсами в определенном контексте.

[294]Key concepts in communication and cultural studies. T. O'Sullivan, J. Hartley, D. Saunders, M. Montgmery, J. Fiske. 2nd ed. Routlege, 1994. P. 92

[295] Cyber protest: new media, citizens and social movements / Ed. By W. van d Donk, B. Loader, P. Nixon, D. Rucht. Routlege, 2004

[296] Rheingold H. The virtual community: Homesteading on the electronic frontier. – MIT press, 1993.

политолог Б. Андерсон, любая нация – «это воображаемая общность»[297], поэтому роль государства в создании и поддержании идентичности чрезвычайно важна. Таким образом, контроль над политической коммуникацией для государства является важным условием политической стабильности.

Под вопросом оказываются эффективность существующих государственных и международных режимов – прежде всего, режима международной электросвязи, регламентирующего потоки трансграничной информации[298].Именно поэтому социокультурное, политико-идеологическое измерение международной информационной безопасности не может быть изъято из международного дискурса и нуждается в регулировании на международном уровне. Таким образом, кибер-подход, т.е. акцент исключительно на технологических аспектах информационной безопасности представляется редуктивным, искажающим действительность. Следовательно, отказ от международных переговоров по данной проблематике ставит под угрозу информационную безопасность как таковую, так как выводит целую сферу за рамки международных договоренностей, провоцируя конфликтность.

Подтверждением тому, что широкое распространение социальных сетевых сервисов и их использование рядом государств во внешнеполитических целях воспринимаются как угроза международной безопасности рядом государств, служит существующая тенденция к фрагментации глобального информационного пространства, вычленения из нее национальных и региональных сегментов. На неформальном саммите ШОС в августе 2011 г. обсуждалась возможность введения информационных границ с целью оградить государства-участники от негативных последствий широкого распространения социальных сетей и их использования государствами в политических целях. Проблематика «цифрового суверенитета» продолжает активно обсуждаться в странах-членах ШОС, а также ряде других государств.

---

[297]См. Anderson B. I. C. Reflections on the Origin and Spread of Nationalism. London: 1983.
[298] Более подробно о режиме международной электросвязи см. в Главе 1.

Основным вызовом международной безопасности, связанным с широким распространением социальных сетевых сервисов и новых медиа, является их использование государствами во внешней политике для реализации внешнеполитических целей в рамках цифровой публичной дипломатии (т.е. направленное воздействие на граждан других государств). Общество становится объектом воздействия посредством социальных медиа. Интернет формирует сложную социальную среду, в которой крайне сложно просчитать последствия принятых решений, поэтому угрозы безопасности, порождаемые использованием инструментов цифровой дипломатии) возрастают (прежде всего, речь идет о дестабилизации социальной ситуации в отдельных странах и регионах). Как отмечается в Доктрине информационной безопасности Российской Федерации, на современном этапе «расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий»[299].

Первыми официальными программами, направленными на использование социальных сетей в Интернете во внешней политике, стали программы цифровой дипломатии США. В настоящее время программы цифровой дипломатии реализуются в большинстве стран мира. По оценкам российских и зарубежных исследователей, именно программы цифровой дипломатии привлекают к себе наибольшее внимание в контексте международной безопасности, так как они

[299] Доктрина информационной безопасности Российской Федерации. Утверждена указом Президента № 646 от 5.12.2016. URL: http://www.scrf.gov.ru/documents/6/5.html

рассматриваются большинством стран как катализатор массовых протестов в странах Ближнего Востока, то есть событий Арабской весны[300].

Как отмечает российский исследователь Н.А. Цветкова, методами цифровой дипломатии являются «размещение радио- и телепередач в сети Интернет, распространение в открытом доступе литературы о США в цифровом формате, мониторинг дискуссий в блог-пространстве, создание персонифицированных страничек членов правительства США в социальных сетях, а также рассылка информации через мобильные телефоны»[301].

Реализация программ цифровой дипломатии правительством США предполагает следующие направления деятельности:

- финансирование проектов по созданию и распространению новых технологий, позволяющих обходить цензуру в Сети;
- создание информационных сервисов, направленных на поддержку оппозиции в авторитарных странах;
- создание систем теневого Интернета и независимых сетей мобильной связи, развертывание которых на территории третьих стран позволит борцам с авторитарными режимами обмениваться информацией он-лайн, обходя запреты властей[302].

«Реализация программ цифровой дипломатии США проводится с опорой на крупные компании Интернет-индустрии. Ключевым для понимания сути цифровой дипломатии является тот факт, что она представляет собой технологический инструмент. В основе внешней политики и цифровой дипломатии Соединенных Штатов заложены идейные основания, которые эффективно воплощает бизнес-модель и информационная политика Google,

---

[300] См. напр.: Морозов Е. Интернет как иллюзия. Обратная сторона сети. – М.: Litres, 2016.; Цветкова Н. А. Социальные сети в публичной дипломатии США //Вестник Санкт-Петербургского университета. Серия 6. Политология. Международные отношения. – 2011. – №. 2.

[301] Цветкова Н. Программы Web 2.0 в публичной дипломатии США // США и Канада: Экономика, политика, культура. 2011. №3. С. 110.

[302] Tech@State // U.S. Department of State: official site. URL:http://www.state.gov/statecraft/tech/index.htm; “Tech@State: Serious Games Conference” Unlocks Human Potential Through Play // Dipnote US: Department of State Official Blog. 6.07.2011. URL:http://blogs.state.gov/index.php/site/entry/techstate_serious_games_conference

Facebook, Twitter и других компаний американской Интернет-индустрии, и ценность демократии и либеральных свобод.

В 2011 г. программы цифровой дипломатии США привлекли к себе существенное внимание, прежде всего, вследствие массовых волн протеста в странах Ближнего Востока и Северной Африки, получивших в прессе название «Twitter-революций» или «Facebook-революций». Был опубликован ряд научных статей, оценивающих роль социальных сетей и новых медиа в так называемой «арабской весне». Движущей силой во всех протестных движениях была молодежь, которая стала совершенно новой, не оформленной идеологически политической силой. При этом была продемонстрирована самостоятельная роль Интернета и СМИ»[303].

Важную роль в направлении и оформлении революций сыграла деятельность внешнеполитических служб США с опорой на социальные сети и новые медиа в Интернете[304]. «Официальная позиция Белого дома по поводу событий «арабской весны» сформулирована в статье главного советника Хиллари Клинтон по инновациям А. Росса. Роль социальных сетей в революционных событиях на Ближнем Востоке оценивается как координирующая, однако не первостепенная[305]. Вместе с тем, в той же статье отмечается трансформирующая роль ИКТ в политике и дипломатии. Утверждается, что они являются важным транслятором идей и способствуют демократизации, как во внутренней, так и в международной политике, хотя и могут использоваться в своих целях диктаторскими и авторитарными режимами»[306].

«Результаты исследования, проведенного в августе 2010 г. Институтом исследований мира США, показывают, что новые медиа оказывают влияние на общественное мнение, смягчают либо обостряют межгрупповые конфликты,

---

[303]Зиновьева Е.С. Цифровая дипломатия, международная безопасность и возможности для России // Индекс безопасности. 2013. № 1. С. 216.

[304]Чернобай А. Роль социальных сетей в мобилизации протестных настроений на Ближнем Востоке и в Северной Африке в в январе-марте 2011 года // Идеологические аспекты военной безопасности. 2011. № 1. URL:http://mod.mil.by/iavb/2011n1/9.pdf

[305]Росс А., Скотт Б. Социальные СМИ: причина, следствие и реагирование // Вестник НАТО. URL:http://www.nato.int/docu/review/2011/Social_Medias/21st-century-statecraft/RU/index.htm

[306]Зиновьева Е.С. Цифровая дипломатия, международная безопасность и возможности для России // Индекс безопасности. 2013. № 1. С. 216.

способствуют коллективным действиям, провоцируют негативную обратную реакцию в государствах с авторитарными режимами, а также привлекают международное внимание к определенным странам. Вместе с тем авторы исследования полагают, что сделать однозначные выводы о влиянии социальных сетей на протесты и революции в странах Северной Африки и Ближнего Востока не представляется возможным. Традиционные СМИ до сих пор являются не менее, а зачастую даже более влиятельными по сравнению с социальными медиа[307]. Исследование «Гражданские инициативы: влияние Facebook и Twitter», проведенное Дубайской школой управления, показывает, что социальные сети, пользователи которых все чаще ставят перед собой политические задачи, сыграли важную роль в мобилизации граждан и формировании общественного мнения. При этом любопытно, что количество пользователей социальной сети Facebook в первые месяцы 2011 г. выросло на 30%[308]. Таким образом, исследователи приходят к схожим выводам о значимом, но не первостепенном влиянии социальных медиа на организацию массовых протестов и революций в странах Северной Африки и Арабского Востока. Также нет единства в оценках роли программ цифровой дипломатии США как катализатора протестных настроений»[309].

Исследователи акцентируют внимание на том, что социальные медиа и Web 2.0 технологии способствуют коллективным действиям, в силу чего они обладают значительным политикообразующим потенциалом, как в рамках отдельного государства, так и на уровне транснациональной политической среды[310]. Таким образом, социальные медиа и Веб 2.0 технологии представляют собой инструменты, который обладают рядом функций в политической коммуникации в глобальном масштабе, – позволяют получить представление о событиях, происходящих в мире, формируют взаимоотношения к тому или иному событию,

---

[307]Aday S. Blogs and bullets. New media in contentious politics // United States Institute of Peace. August 2010. №5. URL:http://www.newmediacenter.ru/wp-content/uploads/2011/10/adayetal2010.pdf

[308] Civil Movements: The Impact of Facebook and Twitter // Arab social media report. May 2011. № 2(1). URL: http://www.dsg.ae/portals/0/ASMR2.pdf

[309]Зиновьева Е.С. Цифровая дипломатия, международная безопасность и возможности для России // Индекс безопасности. 2013. № 1. С. 216.

[310] O'Reilly T., Battelle J. Web squared: Web 2.0 five years on. " O'Reilly Media, Inc.", 2009. 15 p.

позволяют распространять информацию, в том числе культуру, ценности, религию и пр., а также выполняют развлекательную функцию. При этом каждой функции, которые выполняют медиа, есть оборотная сторона, т.е. «дисфункция» (медиа предоставляют информацию людям, которую они впоследствии могут использовать, как на пользу, так и во вред себе и обществу в целом – напр., СМИ распространяют информацию о природном бедствии, чтобы люди имели возможность подготовиться и принять меры, но эта же информация может спровоцировать панику и хаос и др.).

Исследователи связывают мобилизационный потенциал сетевых социальных сервисов с тем, что не только способны изменять иерархический характер коммуникации, характерный для традиционной дипломатии, но и вовлекать рядовых граждан в решение дипломатических задач, а также напрямую обращаться к зарубежной аудитории.Д. Кован и А. Арснольт указывают, что если изначально практика публичной дипломатии обеспечивала переход от монолога к диалогу, то цифровая дипломатия создает также условия для развития проектов сотрудничества, в качестве инструментов могут использоваться различные цифровые платформы для создания контента (wiki-, он-лайн энциклопедии и др.), а также реализация акций и программ, координируемых в он-лайн среде при помощи специальных инструментов краудсорсинга (под краудсорсингом понимается привлечение к решению тех или иных проблем широкого круга лиц, организованных при помощи цифровых площадок коммуникации) и краудфандинга (Под краудфандингом понимается привлечение к решению тех или иных проблем широкого круга лиц, организованных при помощи цифровых площадок коммуникации, которые добровольно предоставляют финансовые средства или другие ресурсы, как напр., платформы ушаиди (ushahidi))[311].

В исследовательском сообществе США отношение к использованию Интернета государственными ведомствами неоднозначно. Преподаватель Джорджтаунского университета Е.Морозов перечисляет угорзы широкого

[311] Cowan G., Arsenault A. Moving from monologue to dialogue to collaboration: The three layers of public diplomacy //The ANNALS of the American Academy of Political and Social Science. 2008. Т. 616. №. 1. P. 10-30.

использования социальных сетей. Web 2.0 усиливает коммуникативную эффективность не только дипломатии, но и различных радикальных организаций[312]. К примеру, можно вслед за многими исследователями отметить усиление позиций политического крыла «Братьев мусульман», что в частности проявилось в их победе на выборах в Парламент Египта в 2012 г. Не последнюю роль в их усилении сыграли как раз социальные сети. Таким образом, социальные сети можно охарактеризовать как амбивалентный инструмент, который в равной степени может усилить как демократические, так и авторитарные тенденции в мире.

Оксфордский университет проводил исследования эффективности программ цифровой дипломатии. В частности, предметом исследования стала речь Барака Обамы в Каире в 2009 г. Контент-анализ обсуждения этой речи в социальных сетях показ, что реакция фокусной общественности на нее была в целом негативной[313].

В последние годы все чаще публикуются работы с пессимистичными оценками роли социальных медиа как факторов разжигания конфликтности, что стало в некоторой степени ответом на события Арабской весны. Высказываются опасения, что социальные медиа могут быть использованы государствами как инструмент дестабилизации ситуации, как в рамках отдельной страны, так и региона в целом. Говоря о влиянии социальных сетей и иных цифровых каналов коммуникации на эскалацию конфликтов, следует отметить целый ряд примеров подобного влияния. Как отмечает политолог Е. Морозов, «В Африке эс-эм-эс часто используются для разжигания вражды. … конфликт мусульман и христиан в нигерийском городе Джос унес жизни более трехсот человек. Правозащитники, изучавшие конфликт в Джосе, собрали по меньшей мере 145 таких сообщений. Одни содержали инструкции по убийству людей и сокрытию их трупов (“Убей,

[312]Morozov E. The Digital Dictatorship // Wall Street Journal. 20.02.2010. URL:http://online.wsj.com/article/SB10001424052748703983004575073911147404540.html

[313] Khatib L. and al. Public Diplomacy 2.0: An Exploratory Case Study of the US Digital Outreach Team // Oxford Internet Institute. CDDRL working papers. 2011. № 120. URL: http://uscpublicdiplomacy.org/media/Exploratory_Case_Study_US_Digital_Outreach_Team.pdf

пока не убили тебя. Закопай, пока не закопали тебя"). С помощью других распространялись слухи, которые привели к эскалации насилия»[314].

Интерактивные Web 2.0 технологии формируют информационный контекст, в котором разворачивается конфликт. Социальные сети способствуют интерактивной коммуникации и распространению информации о конфликтах, создавая возможности для большого количества людей, проживающих в зоне конфликтных действий или вовлеченных в конфликт напрямую передавать информацию о нем для широкой аудитории, расширяя круг косвенных участников конфликта и трансформируя взгляды и предпочтения конфликтующих сторон – то есть, воздействуя на структурные факторы конфликтного противостояния.

При этом объектом цифровой дипломатии становятся не граждане противоположной стороны, а международное общественное мнение. Это тем более парадоксально, потому что объектом цифровой дипломатии в мирное время, как правило, являются общества зарубежных государств. Субъектами же цифровой дипломатии могут быть как государства, так и международные организации, даже отдельные влиятельные лица – например, блоггеры или журналисты. В ходе конфликта стороны апеллируют к международному общественному мнению как внешнему арбитру. Особое внимание, конечно, уделяется институтам и лицам, которые оказывают ключевое влияние на формирование международного общественного мнения. Это ООН, особенно ее генеральный секретарь, международные общественные организации, Папа римский и т.д. Показательно, что выше обозначенные лидеры общественного мнения также представлены в социальных сетях и обладают значительным количеством подписчиков[315].

Принципиальное значение имеет конкуренция или взаимодействие с глобальными СМИ. Информация, распространяемая пользователями социальных

---

[314] Morozov E. The net delusion: The dark side of Internet freedom. Public Affairs, 2012. P. 215.

[315] AFP launches "the e-diplomacy hub", an innovative tool for exploring the world of digital diplomacy. URL: https://www.afp.com/en/agency/press-releases-newsletter/afp-launches-e-diplomacy-hub-innovative-tool-exploring-world-digital-diplomacy

медиа может совпадать, а может и противоречить тому, что говориться на таких «глобальных СМИ», как CNN, BBC, Al Jazeera. Определенное разнообразие в глобальном медийном пространстве позволяет социальным сетям в любом случае доносить свою версию происходящего. Однако если официальные СМИ и социальные медиа формируют определенную медийную картину некоторого события в симбиозе, в этом случае, скорее всего именно эта картина сформирует международное общественное мнение. Например, в ходе протестов в Иране в 2009 году существенную роль в их освещении сыграла социальная сеть микроблоггинга Твиттер, которая по сути сформировала отношение мирового общественного мнения к протестам – значительная часть мировых СМИ перепечатывала сообщения пользователей социальной сети, как выразился Е. Морозов, «мир следил за революцией в Иране через Твиттер»[316]. Центр “Пью рисерч” установил, что 98 % самых популярных гиперссылок, размещенных в “Твиттере” во время беспорядков в Иране, были связаны с этими событиями. Однако, что в большинстве случаев записи в “Твиттере” были сделаны (или продублированы) людьми, находившимися не в Иране[317].

Однако эффективность цифровой дипломатии как инструмента урегулирования конфликтов будет зависеть от чувствительности сторон конфликта к международному общественному мнению, прежде всего, с точки зрения недопустимость жертв среди гражданского населения. Некоторые политические режимы к нему абсолютно равнодушны, другие же напротив – крайне чувствительные. Томас Зейтсофф, профессор школы публичной политики Американского университета, проанализировал на базе обширной статистической информации влияние публикаций в социальных сетях динамику конфликта в Газе в 2012 году[318]. Автор отмечает, что изменения общественного мнения в результате публикаций о насилии в отношении гражданских лиц снижают интенсивность конфликтных действий, прежде всего, это касается Израиля,

[316] Morozov E. The net delusion: The dark side of Internet freedom. Public Affairs, 2012. P. 28.
[317] Там же.
[318] Zeitzoff T. Does social media influence conflict? Evidence from the 2012 Gaza Conflict // Journal of Conflict Resolution. – 2016.

который в большей степени чем ХАМАС, склонен ориентироваться на общественные настроения. Вместе с тем, внимание со стороны посредников - Египта, США, ООН по традиционным каналам дипломатии, а не путем использование социальных сетей, ведет к эскалации конфликта, причем как для Израиля, так и для ХАМАС. Как отмечает автор, и Хамас, и Израиль активно использовали социальные медиа, чтобы оказать влияние на зарубежную аудиторию в ходе этого конфликта. Более того, использование Твиттера обеими сторонами конфликта было беспрецедентным.

Проведенный анализ показывает, что цифровая дипломатия в условиях конфликта будет эффективно снижать его остроту только в случае чувствительности одной из сторон к международному общественному мнению. Исходя из того, что неприемлемость жертв среди гражданского населения является ценностью, характерной для индивидуалистической западной политической культуры, в рамках которой значимы идеалы Просвещения, можно сделать вывод, что использование цифровой дипломатии как инструмента давления будет эффективным в отношении государств, являющихся частью международного сообщества Запада (понимаемого в терминах Х. Булла[319]), или стремящихся войти в него. Это утверждение подтверждается статистикой – более 40% пользователей Твиттера проживает в странах Западной Европы и США[320].

Несмотря на различия политических режимов в чувствительности к международному общественному мнению, практически все они сегодня прибегают к цифровой дипломатии, если для этого есть соответствующие ресурсы. Этим занимается, к примеру, и Хамас, и Израиль. Объясняется это тем, что никто не хочет испытывать дополнительное давление извне. Исключения составляют государства, которые способны обеспечить информационный вакуум для своих граждан, позволяющий последним не замечать внешнее информационное давление, даже если оно возникнет. Но в современном мире сделать это крайне сложно, особенно учитывая практически повсеместное

[319] Bull H. The anarchical society: a study of order in world politics. Palgrave Macmillan, 2012. 329 p.
[320] Jarsky V. How the World Uses Twitter [Infographic] // Marketing Profs. 5.10.2015. URL: http://www.marketingprofs.com/chirp/2015/28385/how-the-world-uses-twitter-infographic

распространение смартфонов, а также планы ряда ИКТ компаний, таких как Google, по созданию инфраструктуры для глобальной зоны беспроводного интернета.

Использование социальных сетей, в том понимании, о котором говорят Д. Кован и А. Арснольт – то есть в целях реализации проектов сотрудничества между конфликтующими сторонами[321], создает возможности воздействия на процедурные факторы конфликта и может быть использовано на этапе миростроительства, создавая, помимо прочего, и возможности по реабилитации сообществ, на значимость чего указывает И.Д. Звягельская[322].

По мнению американского социолога М. Кастельса, широкое распространение социальных сетей и новых медиа и их использование государствами следует рассматривать как источник новых возможностей для развития и разрешения конфликтогенных ситуаций. Глобальные информационные сети и социальные медиа предлагают возможности для формирования гражданского общества и создают площадку для дискуссий. Публичная дипломатия в таком контексте рассматривается не как дипломатия государства, но как народная дипломатия, которая действует поверх межгосударственных отношений и конфликтов, основываясь на общих интересах[323].

Действительно, обсуждение проблем постконфликтного урегулирования на уровне рядовых пользователей Интернета и мобильных телефонов может способствовать укреплению безопасности благодаря формированию атмосферы доверия в международных отношениях. В этом контексте программы цифровой дипломатии способствуют формированию единого информационного пространства, гражданского общества, и разрешения кризисов.

---

[321] Cowan G., Arsenault A. Moving from monologue to dialogue to collaboration: The three layers of public diplomacy // The ANNALS of the American Academy of Political and Social Science. 2008. Т. 616. №. 1. С. 10-30.

[322] Звягельская И.Д. Этноконфессиональные конфликты современности и подходы к их урегулированию. // Конфликты на Востоке: этнические и конфессиональные. / Под ред. А.Д. Воскресенского. М.: Аспект-Пресс, 2008. С. 53.

[323] Castells M. The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance // The Annals of the American Academy of Political and Social Science. 2008. № 616. URL:http://prtheories.pbworks.com/w/file/fetch/45138545/Castells_2008_The_New_Public_Sphere.pdf

Публичная дипломатия – это важный инструмент урегулирования конфликтов, однако, у нее есть свои ограничения. Как отмечает М.М. Лебедева, важно «разводить» воздействие на официальные структуры и публичную дипломатию, предполагающую взаимодействие с общественными организациями, бизнесом, населением государств[324]. Это верно и в отношении цифровой публичной дипломатии. Она не может обеспечить столь же быстрого и явного эффекта, как традиционные дипломатические меры (переговоры о прекращении огня и пр.), однако она также является необходимым инструментом урегулирования современных конфликтов, позволяя сформировать условия для диалога и атмосферу доверия.

В 2012 году было опубликовано исследование ОБСЕ «Подготовка к миру: коммуникации и разрешение конфликтов», в котором, среди прочего рассматривается потенциал социальных медиа и интерактивных он-лайн сервисов в постконфликтном урегулировании. В докладе выделены несколько уровней конфликта, воздействие на которые при помощи каналов социальных медиа может быть эффективным при достижении целей постконфликтного урегулирования:

- индивидуальный уровень – новые медиа создают информационное пространства, в рамках которого их пользователи получают доступ к информации и новостям, а также коммуникативных инструментам, которые способствуют изменению их отношения к предмету конфликта, знаниях и поведении.
- отношения между локальными сообществами – создание Web 2.0 платформ, таких как Peace.Facebook.com, которые способствуют установлению отношений между сообществами, длительное время находившимися в конфликте друг с другом, как израильтяне и палестинцы.
- формирование институтов гражданского общества – распространение социальных медиа облегчает координацию коллективных действий на

[324] Лебедева М.М. Публичная дипломатия в урегулировании конфликтов // Международные процессы. 2017. № 4. С. 45.

уровне гражданского общества, что способствует демократизации и участию различных групп в политическом процессе, содействуя постконфликтному урегулированию[325].

Как отмечают авторы доклада, уже сегодня можно привести ряд примеров, когда социальные медиа используются на уровне сообществ в целях урегулирования конфликтов, их предотвращения или постконфликтного урегулирования по следующим направлениям:

- налаживание межэтнического диалога

Автор приводит в пример создание социальной сети молодых лидеров YaLa-Young Leaders на Ближнем Востоке, которая включает в себя как палестинцев, так и израильтян, что позволяет налаживать связи и устанавливать взаимопонимание «на опережение», предотвращая новый виток конфликтного цикла.

- управление выборами

В Кении и Судане при помощи социальных медиа осуществлялся мониторинг процесса голосования, с целью исключить насилие или мошенничество, информация о которых распространялась при помощи социальных сетей. В обеих странах не так давно прошли референдумы, которые были расценены международными обозревателями как шаг на пути к предотвращению насилия.

- предотвращение криминала и бандитизма

в Бразилии сообщества жителей фавелл («палаточных городов» беднейших жителей) используют социальную сеть Твиттер информирования, что способствует снижению уровня насилия, как со стороны преступных группировок, так и полиции. Аналогичные программы реализуются в Мехико.

- Выработка текста основного закона

В Египте при работе над текстом конституции страны были задействованы все граждане, мнения и предложения которых собирались при помощи

[325] Preparing for peace. Communications in conflict resolution. OSCE Publishing, 2012. URL: http://www.osce.org/networks/98116?download=true

социальных медиа, хотя пример Египта и не является наиболее успешным. Однако аналогичный опыт показал свою эффективность в таких странах, как Марокко и Исландия, и вероятно, будет использоваться в будущем[326].

В силу своей популярности, социальные медиа широко используются на уровне сообществ, а также отдельных лиц, вовлеченных конфликт и заинтересованных в его урегулировании и снижении негативных последствий. Это доступное средство, снижающее стоимость коллективных действий, повышающее эффективность координации, не всегда дает одинаково успешные результаты, однако широко используется и очевидно, что данная тенденция сохранится и будет усиливаться в будущем.

Проведенный анализ показывает, что цифровая дипломатия в условиях конфликта будет эффективно снижать его остроту только в случае чувствительности одной из сторон к международному общественному мнению. С другой стороны, эффективность социальных СМИ как инструментов разжигания и поддержания конфликтов практически не зависит от внешних факторов. Например, социальные медиа играют ключевую роль в практике рекрутирования в ИГИЛ (ДАИШ). Как показывают исследования, данный процесс носит характер самоорганизации. Перебравшись в Ракку молодой житель, например, Лондона активно использует социальные медиа, чтобы обращаться к своим друзьям, близким и знакомым, оставшимся в Великобритании, напоминая им о том, что они мусульмане и должны сражаться за общее дело, что они вместе когда-то давали по этому поводу клятвы и т.д. Как правило, такой призыв от знакомого человека находит отклик и ряды террористов пополняются новобранцами. С другой стороны данные сообщения в социальных сетях, посты с фотографиями, к которым привязаны геотеги, позволяют силам, борющимся с ИГИЛ (ДАИШ), наносит точечные удары по базам боевиков, используя незадачливых блоггеров как наводчиков.

Таким образом, приходится признать, что социальные медиа являются более удобным инструментом для разжигания конфликтов, чем для их

[326] Там же.

урегулирования. Вместе с тем, использование социальных медиа для воздействия на общественное мнение самих конфликтующих сторон может привести к противоположному эффекту. В условиях конфликта высока роль внутригруппового сплочения и внутригрупповой идентификации, поэтому подобная информация может способствовать лишь разжиганию конфликта. В качестве примера можно привести внутренний конфликт в Китае. В 2009 году в китайской провинции Синьцзян интернет был отключен на 10 месяцев в результате массовых столкновений на этнической почве между уйгурами и гоньцами. Поводом к беспорядкам стала провокационная запись на форуме *sg*169.*com*, последующей эскалации насилия способствовал видеоролик, запечатлевший избиение ханьцами нескольких уйгуров-рабочих толпой, вооруженной металлическими трубами[327].

Однако, использование данных цифровой коммуникации и их анализ позволяет снизить напряженность и обратить вспять развитие конфликта, зачастую это достигается отключением коммуникаций. Как отмечает уже упоминавшийся Е. Морозов. в ходе конфликта в Кении социальные сети и мобильная телефония использовались для того, чтобы сперва собирать конфиденциальную информацию о представителях отдельных этнических групп, а затем распространять ее, чтобы нападать на них и запугивать. “Кровь невинных кикуйю больше не будет литься! Мы перебьем врагов прямо тут, в столице. Во имя справедливости запишите имена всех луо и калео, которых знаете на работе, на участке, вообще в Найроби, и не забудьте, какой дорогой их дети добираются в школу. Мы укажем номер, на который нужно отправлять эти сообщения”, – гласило э-эм-эс. Кенийские власти тогда решили отключить мобильные сети, чтобы избежать эскалации насилия, что способствовало снижению насилия, но не смогло предотвратить негативных последствий конфликта - от восьмисот до полутора тысяч человек погибло, около 250 тысяч покинули свои дома[328].

[327] Morozov E. The net delusion: The dark side of Internet freedom. Public Affairs, 2012. P. 13.
[328] Там же. P. 215.

Таким образом, первоначальный оптимизм относительно способности социальных медиа содействовать демократизации и, как следствие, снижению конфликтности во всем мире, впоследствии сменился более критичными оценками.

Современное обострение отношений России со странами Запада, связанное с воссоединением с Крымом, также сопровождается информационным противостоянием, которое транслируется в социальные сети. В частности, США спонсировали создание в 2015 г. цифрового медиа департамента на базе чешского офиса радио «Свобода», в котором будут работать специалисты по социальным сетям, чья задача «противостоять дезинформации в российской медиасфере посредством различных социальных медиа (в частности, Facebook, Twitter, «ВКонтакте» и «Одноклассники»)»[329]. Схожие задачи, на уровне СМИ и социальных медиа, в рамках Европейского союза ставятся перед East StratComTeam – специальной командой, состоящей из экспертов и чиновников внешнеполитической службы ЕС[330]. Таким образом, наметилась гонка не только кибер-вооружений, но и информационных. Как отмечает российский исследователь Н.А. Цветкова, в последние годы наметилась концептуальная трансформация подхода США к использованию интернет-технологий в транснациональной политической коммуникации. Новая концепция, получившая название диалоговой пропаганды / стратегической коммуникации предполагает более выраженный пропагандистский характер и лучше приспособлена «к условиям открытой информационной войны, когда четко определены мишени, а инструменты стратегической коммуникации подчинены одной цели – идеологической ликвидации конкурентов США»[331].

Таким образом, несмотря на первоначальный оптимизм относительно демократизирующего потенциала интернета и социальных медиа, современные исследования показывают, что популярность Интернет-коммуникации создает

---

[329] СМИ: Соединённые Штаты направляют в российские соцсети информационные войска // RT на русском. 14.04.2015. URL: http://russian.rt.com/article/85463

[330] Дудина Г. Война до победного словца // Коммерсант. 23.08.2015. URL: http://www.kommersant.ru/doc/2795055

[331] Цветкова Н.А. Публичная дипломатия США: от «мягкой силы» к «диалоговой пропаганде» // Международные процессы. 2015 № 3. С. 131. URL: http://www.intertrends.ru/forty-second/Tsvetkova_42.pdf

опасность поляризации и раскола, как в рамках отдельных обществ, так и на глобальном уровне. Как показывают социологические исследования, пользователи социальных сетей, таких как Twitter, Facebok и др., склонны к радикализации мнений и формированию изолированных Интернет-сообществ[332]. В 2000 году Р. Патнэм предостерегал о возможности «киберапартеида» и «кибербалканизации»: «политическая культура Интернета по своей сути либертарианская и по многим аспектам Интернет представляет собой естественное состояние в Гоббсианском, а не Локковском смысле»[333]. Другие социологи высказывали схожие опасения, в том числе М. Кастельс[334]. К. Санстейн утверждал, что «новые технологии, прежде всего Интернет, усилили способность людей слышать только свой собственный голос и отгораживаться от других»[335].

В последние годы внимание исследователей, занимающихся проблематикой политического использования социальных медиа, отходит от событий арабской весны. Так, в мае 2015 года вышел специальный номер журнала Исследования мира, посвященный исследованию коммуникаций, технологий и политических конфликтов. Значительная часть статей, опубликованных в этом номере, прямо или косвенно затрагивает проблематику роли социальных медиа в современных международных конфликтах. Н. Вейдман отмечает, что широкое распространение социальных сетей способствует эскалации насилия в вооруженных конфликтах[336].

Т. Варрен доказывает данный тезис на основании эмпирического анализа вооруженных конфликтов в странах Африки доказывает, что распространение массмедиа (коммуникация по типу один-ко-многим) способствует развитию связей между гражданами и государством, что снижает уровень коллективного насилия, в то время как распространение социальных медиа в регионах с

[332] Sustein J. Public.com 2.0. NJ: Rincenton University Press, 2007. P. 56
[333]Цит. по: Drezner D. W., Farrell H. Introduction: Blogs, politics and power: a special issue of Public Choice // Public Choice. 2008. №. 1-2. P. 1.
[334] Castells M. The network society //London, 1996.P. 107.
[335] Sunstein C. The daily we: Is the internet really a blessing for democracy //Boston Review. 2001. №. 3.
[336] Weidmann N. Communication networks and the transnational spread of ethnic conflict // Journal of Peace Research. 2015. № 3 (52).

отсутствием доступа к массовым медиа способствует увеличению уровня насилия[337].

Социальные сети способствуют интернационализации конфликтов и их распространению на другие государства, так как информация о насилии провоцирует внутригосударственных акторов в других государствах за счет демонстрационного эффекта, причем географическая близость между странами не так важна, как наличие налаженных коммуникаций между населением и лидерами этнических групп. Кроме того, наличие каналов коммуникации, с помощью мобильных телефонов и социальных медиа, как отмечает К. Байлард, вооруженные группировки могут повысить эффективность коллективных действий за счет дешевой и оперативной коммуникации, а также повышают склонность группы к самоорганизации благодаря более эффективной коммуникации об общих проблемах и недовольствах[338].

Т. Зейтсофф доказывает, что социальные медиа используются не только для внутригрупповой коммуникации конфликтующих сторон, но и для взаимодействия с более широкой международной аудиторией. Исследуя роль социальных сетей в конфликте Израиля и ООП, он отмечает, что рост внимания международных акторов, США, Египта, ООН усиливает интенсивность конфликта как со стороны Израиля, так и ООП[339].

Вместе с тем, осуждение со стороны международной аудитории способствует более сдержанному поведению со стороны Израиля, и более агрессивному со стороны Хамас. Таким образом, начинает формироваться предметная область исследований, посвященная изучению роли социальных медиа в современных конфликтах. Большинство исследователей отмечает значимую роль социальных сетей в эскалации конфликтов, прежде всего, внутригосударственных. Как отмечают российские исследователи М.М. Лебедева,

---

[337]Warren T. Explosive connections? Mass media, social media, and the geography of collective violence in African states // Journal of Peace Research. 2015. № 3 (52).

[338] Bailard K. Ethnic conflict goes mobile: Mobile technology's effect on the opportunities and motivations for violent collective action // Journal of Peace Research. 2015. № 3 (52). Pp. 323-337

[339] Zeitzoff T. Using Social Media to Measure Conflict Dynamics: An Application to the 2008-2009 Gaza Conflict // Journal of Conflict Resolution.2011. № 55(6). Pp. 938-969

М.В. Харкевич, Е.С. Зиновьева и Е.Н. Копосова, «в условиях слабых государственных институтов деструктивная роль интернет-коммуникации усиливается. Информационные технологии, особенно Web 2.0, способны стимулировать откат к политической архаике. Под политической архаикой понимается возвращение к неформальным институтам и практикам, основанным на потестарности, криминале, религии, родственности и клановости особенно подвержены архаизации слабые султанистские режимы. Массовое распространение в них Интернета приводит к нарастанию потенциала протестных движений, при этом слабые государственные институты не могут эффективно контролировать данные настроения. В результате возрастает вероятность выплеска на улицы хорошо организованного и скоординированного благодаря технологиям Web 2.0 протеста, требующего либерализации политической жизни в стране. В этом случае государство скорее всего обречено на архаизацию. Попытки подавить протестное движение могут привести к гражданской войне, которая в условиях слабости государственных институтов, вероятно, завершится окончательным “провалом” государства. В случае выполнения требований протестующих либерализация будет происходить в условиях слабости государственных институтов, что тоже способно привести к архаизации государства. Вероятность архаизации государственных институтов особенно высока на Ближнем Востоке и в Северной Африке, так как там наслаиваются сразу два кризиса – на глобальном и региональном уровнях. На глобальном уровне продолжается эрозия фундаментальных институтов Вестфальской политической модели мира, на региональном – кризис идентичности, связанный с исчезновением оппозиции “социализм – капитализм” времен холодной войны и усилением роли политического ислама, подрывающего легитимность стареющих светских режимов»[340].

В этих условиях возникает опасность фрагментации Интернета, распада на независимые сегменты, управляемые суверенными государствами. Фрагментация

[340] Лебедева М. М., Харкевич М. В., Зиновьева Е. С., Копосова Е. Н. Архаизация государства: роль современных информационных технологий. – Полис. Политические исследования. 2016. № 6. С. 22-36.

возможна либо за счет формирования закрытых внутригосударственных цифровых пространств, либо формирования параллельных проектов глобальной сети за счет создания альтернативной системы доменных имен на базе регионов, транс региональных объединений государств или отдельных стран[341]. Число государств, принимающих ограничительные меры в отношении национальных сегментов Интернета, возрастает. При этом современная система управления интернетом, в рамках которой координация технической инфраструктуры сети обеспечивается некоммерческой структурой, зарегистрированной в США, усугубляет опасения государств в том, что интернет-коммуникации могут быть использованы как инструмент вмешательства во внутренние дела, что, в свою очередь политизирует международный режим управления интернетом.

Вместе с тем, ограничение доступа к Интернету и социальным сетевым сервисам не означает стремления к полной изоляции от глобальных информационных потоков. Журналист и исследователь Б. Ристоу выделяет тенденцию к усложнению практики государственного регулирования Интернета. Правительства становятся более искушенными и уже не заинтересованы в полном блокировании трафика: скорее, они хотят предоставить гражданам некую форму управляемого доступа и за счет этого иметь возможность отслеживать их настроения и поведение в Сети[342].

Иной взгляд на проблему можно обнаружить у классика исследований информационного общества М. Кастельса. В распространении социальных сетей он видит скорее не угрозу международной безопасности, а возможность решения глобальных проблем, которые превосходят по своим масштабам возможности любого отдельного государства. Информационные сети создают условия для развития действительно глобального гражданского общества, а также для поддержания глобального диалога. Публичная дипломатия превращается в этом

---

[341] См.: The future of the internet. A virtual counter-revolution // Economist. 2.09.2010. URL:http://www.economist.com/node/16941635

[342] Ristow B. The New Gatekeepers: Controlling Information in the Internet Age. A report to the Center for International Media Assistance // Center for International Media Assistance. 2013. URL: http://apo.org.au/files/Resource/CIMA_TheNewGatekeepers_May2013.pdf

случае из межгосударственной в международную в буквальном смысле этого слова[343].

Тем не менее, информационная сфера не свободна от межгосударственных противоречий. М. Кастельс отмечает, что сегодня борьба за власть в глобальной информационной сфере обострилась. Примерами такого обострения могут выступать цензурирование электронной почты в Китае; активное законодательное регулирование информационной сферы в Европейском союзе и т.д[344].

Наиболее важным ресурсом «мягкой силы» в мировой политике сегодня является информация. «Мягкая сила» основана на и реализуется только в рамках коммуникации. В свой книге о будущем власти Дж. Най, автор концепции «мягкая сила», делает вывод, что в эпоху информационной глобализации власть видоизменяется, ее основным ресурсом перестает быть военная сила и становится информация. «В век информации может победить тот, кто способен представить себя в лучшем свете»[345]. На это направлены программы цифровой дипломатии Соединенных Штатов. При этом современные социальные медиа в сочетании с возможностями машинного анализа «больших данных» предоставляют уникальные возможности политического влияния. Технология микротраргетирования которая изначально применялась в маркетинге, сегодня играет значимую роль в политике, в особенности, в избирательных кампаниях (под микротаргетированием понимается «сегментация целевой аудитории с использованием уникального алгоритма, который определяет комбинацию демографических и психографических характеристик для каждого из сегментов»[346]) позволяет существенно повысить эффективность воздействия на избирателей за счет донесения персонализированной и интерактивной информации посредством социальных сетей и иных каналов интернет-коммуникации. Эту технологию широко использовал в своей предвыборной

---

[343] Castells M. The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance // The Annals of the American Academy of Political and Social Science. 2008. № 616.
URL:http://prtheories.pbworks.com/w/file/fetch/45138545/Castells_2008_The_New_Public_Sphere.pdf
[344]Там же.
[345] Nye J. The future of power. N.Y.: Basic Books, 2011. 300 p.
[346] Северс А.В. Стратегия микротаргетирования и роль социальных сетей в политических коммуникациях // Вестник Московского университета. Серия 10. Журналистика. 2013. № 2. С. 38.

кампании Б. Обама, однако наиболее широкую известность приобрела кампания действующего президента США Д. Трампа, в которой эти технологии были использованы масштабно и по оценкам аналитиков, весьма эффективно[347].В виду новизны и динамичного развития данной технологии, в открытой печати не удалось найти исследований, статистически оценивающих эффективность микротаргетирования в рамках политической деятельности, вместе с тем, как представляется, использование данной технологии во внешней политике государств в рамках программ цифровой дипломатии может создать новое измерение угроз международной информационной безопасности, связанных с возможностью трансграничного влияния на общественное мнение и политические предпочтения людей.

Неудивительно, что расширение возможностей США в области глобального информационного влияния за счет использования средств информационного воздействия и цифровой дипломатии, опирающейся на возможности социальных сетей Web 2.0 технологий, порождает у менее продвинутых в этой сфере государств ощущение уязвимости и желание отгородиться от глобального информационного пространства, а также создавать собственные информационные средства воздействия, в том числе принимать программы ведения информационных войн. Ситуация усугубляется за счет того, что государства рассматривают программы цифровой дипломатии США как попытку вмешательства во внутренние дела, угрожающую нарушением их государственного суверенитета»[348]. Наличие таких опасений подтверждают регулярные попытки закрыть доступ к сервисам Facebook, YouTube, Blogspot – в разные периоды времени они были заблокированы во Вьетнаме, Иране, Саудовской Аравии, Египте, Пакистане, Мьянме, Северной Корее и ряде других стран[349].

---

[347] См. напр.: Роговский Е.А. Выборы в США: успех технологических инноваций // Международная жизнь. 2017. №3. С. 107-122.

[348]Зиновьева Е.С. Цифровая дипломатия, международная безопасность и возможности для России // Индекс безопасности. 2013. № 1. С. 216.

[349]Freedom on the Net. A Global assessment of Internet and Digital Media // Freedom House. 01.04.2009. URL:http://www.state.gov/documents/organization/135959.pdf

Показательно, что аналогичной позиции придерживается Российская Федерация. Согласно принятому в 2013 г. документу «Основы государственной политики в сфере информационной безопасности до 2020 г.» в дополнение к широко признанной в российской политике и дипломатии «триаде угроз» международной информационной безопасности, которая включает в себя террористическую, преступную и военно-политическую, была указана четвертая – использование Интернет-технологий для «вмешательства во внутренние дела государств», «нарушения общественного порядка», «разжигания вражды», «пропаганды идей, подстрекающих к насилию». Подразумевается поддержка использования социальных сетей для организации антиправительственных акций[350].

Развитие информационных технологий, в том числе социальных сетей, создает новые технологии для реализации внешнеполитических целей, усиления «мягкой» и жесткой силы государства. При этом однозначно разделить «мягкую» и жесткую силу в информационном пространстве невозможно. Манипуляция социальными сетями позволяет использовать уязвимости национальной и международной безопасности, усиливающиеся вследствие процессов глобальной информатизации. Контент социальных медиа, направленность дискуссии, ее тональность, повестка дня поддаются манипулированию. Источники манипулирования социальными медиа в силу их транснационального характера зачастую может находиться за пределами того государства, чье общество выступает в роли объекта манипуляции. Как отмечает один из американских теоретиков информационного общества Р. Шафрански «демократические социальные системы могут быть несколько более устойчивыми к выводу из строя по сравнению с тоталитарными политическими режимами»[351]. Открытое информационное общество, как общество, основанное на знаниях, является более устойчивым к информационному манипулированию, но не обладает абсолютным иммунитетом. Вместе с тем, по мере развития информационного общества более

[350] Черненко Е.В. Мир домену твоему. Россия определилась с политикой информационной безопасности // Коммерсантъ. 01.08.2013. № 135 (5166). URL:http://www.kommersant.ru/doc/2245463
[351] Szafranski R. A Theory of Information Warfare: Preparing for 2020 / Airpower Journal, 1995 №1.

уязвимыми становятся критические информационные инфраструктуры, прежде всего в экономическом измерении.

2.4. Политические проблемы применимости международного права к информационной сфере

«Можно выделить несколько ключевых особенностей информационной сферы в целом и конфликтов в частности, оказывающих существенное влияние на применимость международно-правовых норм к данной области:

- защищенные и незащищенные объекты критической инфраструктуры в информационном пространстве тесно переплетены между собой;

- гуманитарные объекты критической информационной инфраструктуры не обладают отличительными знаками, отмечающими их особый правовой статус;

- в информационной войне сложно провести разделение между гражданскими и военными целями;

- влияние негосударственных участников и неправительственных акторов в информационной сфере сопоставимо с государственной мощью;

- информационное оружие обладает характеристиками, отличающими его от традиционных вооружений, вследствие чего его действие частично выпадает из сферы действия международного гуманитарного права;

- информационная война может вестись без предупреждения, сложно определить инициаторов информационной атаки, однозначно оценить масштаб ущерба, а также меру ответного удара; применять традиционные механизмы сдерживания.

- международно-правовое регулирование информационной войны необходимо для сохранения сложившейся системы международной безопасности»[352].

Вследствие вышеперечисленных особенностей ИКТ возникает целый ряд проблем, связанных с применимостью международного права к информационной

[352] Коротков А.В. Безопасность критических информационных инфраструктур в международном гуманитарном праве / А.В. Коротков, Е.С. Зиновьева // Вестник МГИМО-Университета. - 2011. - № 4. - С. 154-162

сфере в контексте ее безопасного развития. Ниже перечислены основные сложности (сгруппированные в пять проблемных областей), связанные с международно-правовым регулированием информационного пространства, которые, в свою очередь, являются препятствием для развития международного сотрудничества по обеспечению информационной безопасности и обуславливают специфику информационной безопасности как объекта регулирования на международном уровне.

Специфика угроз международной информационной безопасности

1. Связь между злонамеренным использованием ИКТ и нарушением территориальной целостности и политической независимости, также как нарушением суверенитета далеко не всегда является очевидной.

2. Трактовка понятия «территориального суверенитета» применительно к злонамеренному использованию ИКТ не является очевидной. Даже если компьютерные и телекоммуникационные устройства, другие средства вычислительной техники расположены на территории того или иного государства, объем его компетенции в рамках суверенитета не является абсолютным.

3. Агрессивные действия государств в информационном пространстве могут маскироваться под хакерские и террористические атаки. При этом хакерские, террористические или криминальные атаки с использованием информационного оружия не подпадают в сферу действия международного публичного права.

4. Анонимность и доступность ИКТ затрудняют однозначное определение источника информационной атаке и могут привести к приписыванию факта применения силы государству или негосударственному актору, чьи информационные системы ресурсы были использованы без его ведома.

Проблемы адаптации норм международного права, регламентирующих применение силы, к информационному пространству

1. В международном праве не выработаны общепризнанные понятия войны или вооруженного конфликта, тем более не существует нормативно признанных определений войны в информационной сфере. Рассмотрение информационной

войны и выработка особого определения необходимы в силу того, что она обладает рядом особенностей по сравнению с военными действиями в «реальном» мире:

- отсутствие предвоенного периода, следовательно, невозможность определения начала войны,
- трансграничность, то есть возможность проведения агрессивных действий в отношении противника без физического пересечения границ его территории
- ИКТ по умолчанию не являются оружием и могут быть отнесены к объектам двойного назначения, что создает сложности с точки зрения классификации использования ИКТ в военно-политических, террористических или преступных целях в качестве акта агрессии[353].

2. Возникают проблемы с классификацией злонамеренного использования ИКТ как агрессии в соответствии с резолюцией ГА ООН 3314 «Определение агрессии» от 1974 г. В соответствии со статьей 2 данного документа квалификация действий государств как агрессии проводится на основании принципа первенства, критериев опасности и враждебности, независимо от того, была ли объявлена война[354]. Данные положения применимы к информационной сфере, однако отдельные нормы документа нуждаются в адаптации к новым реалиям информационного века. В отличие от традиционного понимания агрессии, информационное воздействие не предполагает введение информационных сил на территорию жертвы агрессии и физического нарушения государственного суверенитета.

4. Реализация права на самооборону в информационном пространстве затруднена в условиях отсутствия критериев обоснования оправданности и пропорциональности ответных действий, принципов идентификации агрессора. Остается открытым вопрос о предотвращении злоупотреблений правом на самооборону и коллективную оборону в ответ на информационные атаки.

---

[353] Крутских А.В., Стрельцов А.А. Международное право и проблема обеспечения международной информационной безопасности // Международная жизнь. 2015. № 4. URL: https://interaffairs.ru/jauthor/material/1167

[354] Определение агрессии. Утв. резолюцией 3314 (XXIX) ГА ООН. Нью-Йорк, 14.12.1974. URL: http://www.un.org/ru/documents/decl_conv/conventions/aggression.shtml

5. В случае информационной атаки сложно оценить физический ущерб, так как зачастую издержки носят нематериальный, однако не менее чувствительный характер (например, утечки секретной информации на сайте WikiLeaks или в результате актов кибершпионаза). В этих условиях с целью обеспечить информационную безопасность и предотвратить дальнейшую милитаризацию информационного пространства необходимо на международном уровне согласовать пороговый уровень ущерба, после которого можно квалифицировать использование информационного оружия как вооруженную агрессию.
5. Отсутствие прецедентов и международно-правовой базы затрудняет международное правосудие в сфере ИКТ. В настоящее время государство, ставшее объектом информационной атаки не может подать жалобу в Международный суд, так как в условиях отсутствия международно-правовых актов, регламентирующих данную сферу и судебных прецедентов, не определены необходимые фактические доказательства атаки и критерии их объективности и достоверности.
6. Согласно обычному международному праву государство несет ответственность за деятельность органов государственной власти, а также лиц, действующих под их контролем. Определить, действует ли определенное лицо в киберпространстве под контролем государства, может быть непросто. По мнению части экспертов, применение силы против субъекта на территории иностранного государства возможно, только если данный субъект действует под контролем государства либо с его попустительства (т.е. государство, с территории которого действует субъект, «не способно или не желает» принять меры против него).
7. «Актуальной правовой проблемой также является реализация права государств на нейтралитет, в случае если их информационные системы используются третьими странами для осуществления информационных атак или иных противоправных действий»[355].

[355] Крутских А.В., Стрельцов А.А. Международное право и проблема обеспечения международной информационной безопасности // Международная жизнь. 2015. № 4. URL: https://interaffairs.ru/jauthor/material/1167

Адаптация международного гуманитарного права к информационному пространству.

В связи с развитием ИКТ в серьезной адаптации нуждаются нормы международного гуманитарного права. Международное гуманитарное право предполагает обеспечение безопасности гражданского населения и защиту объектов, ключевых для безопасности гражданских. К сфере гуманитарного права в связи с использованием в вооруженных конфликтах ИКТ относится целый ряд вопросов, представленных ниже.

1. Встает вопрос о критериях отнесения информационных инфраструктур к гражданским / военным объектам, что осложняется тем фактом, что большинство критических информационных инфраструктур являются объектами двойного назначения, и могут быть использованы как в гражданских, так и в военных целях.
2. Согласно нормам международного гуманитарного права необходимо обеспечить соблюдение принципов пропорциональности и избирательности при проведении атак, однако в информационном пространстве применение данного принципа представляется затруднительным.
3. Принимая во внимание анонимность и доступность ИКТ в условиях информационного конфликта сложно разграничить комбатантов и нонкомбатантов.

Обозначенные проблемные вопросы осложняют применимость норм международного гуманитарного права к информационному пространству и обуславливают потребность в выработке новых правовых норм.

Частные вопросы применения международного права к информационному пространству

1. Является ли концепция «территориального суверенитета» основанием для отказа от поиска путей решения проблемы интернационализации управления Интернет и, в частности, ограничения суверенитета США в области

регулирования и применения права в отношении провайдеров сети Интернет, оказывающих услуги с использованием рутовых сайтов сети.

2. Проникновение ИКТ во все сферы жизни общества и государства ставит задачу поиска оптимального баланса между безопасностью и свободой, правом на доступ к информации и ответственностью государств за действия в глобальном информационном пространстве. Согласно Докладу Группы правительственных экспертов ООН по МИБ 2010 гг. государственные усилия по обеспечению информационной безопасности должны идти рука об руку с защитой прав человека и фундаментальных свобод[356]. Кибер-шпионаж, покушение государства на частную жизнь пользователей Интернета, о чем стало известно в результате разоблачений Э. Сноудена, представляет собой реальную угрозу информационной безопасности и актуализирует выработку норм защиты прав человека и защиты данных в информационном пространстве.

Международно-правовые меры предупреждения конфликтов с использованием ИКТ

Среди средств предупреждения злонамеренного использования ИКТ в военно-политических целях обычно выделяют создание обстановки стратегической стабильности, в том числе, посредством транспарентности, взаимодействия, включая меры доверия, и меры по стабилизации.

Для обеспечения международной безопасности и стабильности «необходимо закрепить обязанность государств воздерживаться от атак на критические информационные инфраструктуры. Но реализация подобного обязательства требует идентификации подобных инфраструктур, определения критериев отнесения тех или иных объектов к критическим национальным или международным инфраструктурам»[357]. Идентификация критических информационных инфраструктур не может не поставить под угрозу безопасности

[356] General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/65/201, 30 July 2010.

[357] Крутских А.В., Стрельцов А.А. Международное право и проблема обеспечения международной информационной безопасности // Международная жизнь. – 2015. - № 4. – URL: https://interaffairs.ru/jauthor/material/1167

государства, так как это по сути означает раскрытие наиболее уязвимых для атаки сегментов национального сегмента информационного пространства[358].

Подводя итог, можно отметить, что ИКТ настолько динамичны, что правовые нормы не всегда «успевают» адекватно отразить информационную реальность. Тем не менее, это не отменяет регламентацию межгосударственных отношений нормами международного публичного права. Однако многие из его положений были разработаны применительно к традиционным войнам и требуют доработки, если не по духу, то по форме. Недостаточность международно-правовой базы затрудняет развитие и углубление международного сотрудничества. Однако политика в информационном обществе играет не меньшее значение, чем в реальном мире, следовательно, политизируется и вопрос о применимости международного права к информационному противоборству.

В существенной доработке нуждаются «нормы международного гуманитарного права. В отдельных случаях необходима выработка новых правовых норм, регламентирующих отношения, возникающие в информационном пространстве. Необходимо также выработать систему мер по адаптации общепризнанных принципов и норм международного права к специфике безопасности в сфере использования ИКТ»[359].

Международное гуманитарное право разрабатывается государствами, которые являются не только субъектами права, но и могут быть легитимными участниками военных действий. ИКТ создают новую «территорию», в которой на равных действуют государства и негосударственные акторы, а провести разделительную черту между комбатантами и нонкомбатантами крайне сложно.

В информационной сфере сложно разграничить гражданские и военные элементы критических информационных инфраструктур. К военным относятся объекты, «которые в силу своего характера, размещения, назначения или использования вносят эффективный вклад в военные действия и полное или

---

[358] Коротков А.В. Безопасность критических информационных инфраструктур в международном гуманитарном праве / А.В. Коротков, Е.С. Зиновьева // Вестник МГИМО-Университета. - 2011. - № 4. - С. 154-162

[359] Крутских А.В., Стрельцов А.А. Международное право и проблема обеспечения международной информационной безопасности // Международная жизнь. – 2015. - № 4. – URL: https://interaffairs.ru/jauthor/material/1167

частичное разрушение, захват или нейтрализация которых при существующих в данный момент обстоятельствах дает явное военное преимущество»[360]. Это утверждение верно и в отношении критических информационных инфраструктур, широко используемых в мирное время.

Анонимность ИКТ и, как следствие, сложность идентификации агрессора могут привести к приписыванию факта применения силы государству, чьи информационные системы были использованы для осуществления атаки без уведомления. Как представляется, использование территории третьего государства без его ведома с целью осуществления информационной атаки влечет за собой его вовлечение в конфликт, но не перенесение на него ответственности за агрессию. Необходима выработка соответствующих международно-правовых норм и мер доверия, что предполагает интенсификацию международного взаимодействия государств и перевод его на новый, более высокий уровень сотрудничества в области информационной безопасности.

Особые характеристики ИКТ не означают, что их военно-политическое использование находится в соответствии с международным правом, прежде всего, с Уставом ООН. При этом вытекающие из Устава ООН общепризнанные принципы международного права, а именно невмешательство во внутренние дела государств и неприменение силы и угрозы силой, равно применимы как к традиционной международной политике, так и межгосударственным отношениям в цифровом пространстве[361].

Вышеуказанные проблемы лежат в основе межгосударственных дискуссии по вопросам информационной безопасности, и их разрешение на экспертном уровне могло бы создать основу для развития сотрудничества. В этих условиях актуализируется роль таких негосударственных акторов, как исследовательские сообщества, которые выполняют функции определения областей совпадающих интересов, что затем может лечь в основу международной повестки дня.

---

[360]Второй протокол к Гаагской конвенции о защите культурных ценностей в случае вооруженного конфликта 1954 года. Гаага, 26 марта 1999 г. (ст. 1).

[361] Зиновьева Е. Международное сотрудничество по обеспечению информационной безопасности // Право и управление. XXI век. - 2014. - № 4.

Вывод по главе:

Анализ существующих угроз международной информационной безопасности показывает, что в цифровую эпоху сущность безопасности не поменялась – определение А. Уолферса, согласно которому национальная безопасность определяется как отсутствие угроз ключевым ценностям общества[362],остается верным. Однако изменились условия и средства обеспечения безопасности, характер вызовов и угроз; трансформации претерпевает также состав и характер взаимоотношений между субъектами обеспечения безопасности. Важно учитывать природу этих изменений, для того чтобы адекватно выстраивать механизмы обеспечения информационной безопасности на международном уровне.

Можно выделить несколько ключевых особенностей информационной сферы в целом, которые, в свою очередь, оказывают воздействие на природу международного сотрудничества в данной области:

- транснграничный характер информационного пространства и взаимозависимость государств в данной сфере усиливают уязвимость государств и негосударственных акторов;

- влияние негосударственных участников и неправительственных акторов в информационной сфере выше, чем в большинстве других областей мировой политики;

- защищенные и незащищенные объекты критической инфраструктуры в информационном пространстве тесно переплетены между собой, в информационной войне сложно провести разделение между гражданскими и военными целями, что осложняет регламентацию данной области и ведет к тому, что информационные атаки могут осуществляться в мирное время, как часть межгосударственной конкуренции;

[362] Wolfers A. " National Security" as an Ambiguous Symbol // Political Science Quarterly. 1952. P. 482.

- информационная война может вестись без предупреждения, сложно определить инициаторов информационной атаки, однозначно оценить масштаб ущерба, а также меру ответного удара; применять традиционные механизмы сдерживания.

Выше обозначенные особенности затрудняют международное сотрудничество по обеспечению информационной безопасности, так как они создают сложности в отношении мониторинга достигнутых договоренностей и оценки намерений участников международного взаимодействия (в силу сложности атрибуции информационной атаки и оценки масштаба ущерба). Выше обозначенные факторы, как отмечал авторитетный исследователь реалистского толка Д. Грико, являются существенными препятствиями для международного сотрудничества[363]. Однако, как убедительно доказывает Д. Фирон, несмотря на значимость специфики объекта регулирования, наибольшее влияние на природу и перспективы международного сотрудничества оказывает стратегическая структура международного взаимодействия в исследуемой области и восприятие значимости проблематики субъектами взаимодействия.

Отметим, что сегодня выделяют три основные группы угроз международной информационной и кибербезопасности, определяемые по характеру целеполагания их субъектов – информационная преступность, информационный терроризм и межгосударственные информационные войны и конфликты. При этом большинство исследователей согласны с тем, что, несмотря на значимость первых двух, именно военно-политическое измерение информационной безопасности представляет наибольшую угрозу международному миру и стабильности. Ключевая роль военно-политического измерения информационной безопасности подтверждает, что данная сфера является секьюритизированной, то есть приоритетной для субъектов международного сотрудничества, что, следовательно, предопределяет сложный и длительный переговорный процесс. На сегодняшний день одним из ключевых

[363] Grieco J. M. Anarchy and the limits of cooperation: a realist critique of the newest liberal institutionalism //International organization. 1988. Т. 42. №. 03. С. 485-507.

противоречий, препятствующих формированию режима информационной безопасности на глобальном уровне, являются противоречия в терминологии.

В настоящее время можно выделить два конкурирующих секьюритизирующих дискурса в области информационной безопасности, по-разному определяющих природу и характер угроз национальной и международной безопасности в условиях глобального информационного общества. Эти два дискурса связаны с расхождениями в подходах государств к определению угроз в сфере ИКТ, подлежащих урегулированию на международном уровне, но они широко представлены также и в исследовательской литературе. Дискурс «кибербезопасности», в рамках которого в роли секьюритизирующих акторов выступают в основном государства Запада, а в роли функциональных акторов – бизнес-структуры, ориентированные на выход на глобальные рынки, ориентирован на обеспечение информационно-технической безопасности, что включает в себя защиту, контроль и соблюдение законности и правопорядка в телекоммуникационной сфере. Дискурс «информационной безопасности», в рамках которого в качестве секьюритизирующих акторов выступают страны БРИКС, ряд арабских государств и в качестве функциональных акторов - бизнес-структуры, ориентированные на внутренние рынки этих стран и предполагает обеспечение не только информационно-технической, но и информационно-психологической безопасности, что подразумевает защиту психологического состояния общества и государства от негативного информационного воздействия.

В рамках информационно-технического измерения международной информационной безопасности особую опасность представляют угрозы критической информационной инфраструктуре государства, что может создать реальную угрозу национальной и международной безопасности не только в виртуальном, но и в реальном мире.

В рамках социо-гуманитарного измерения международной информационной безопасности актуализируется дискурс о возможном использовании социальных медиа как каналов информационного воздействия.

Таким образом, возрастающая зависимость всех сфер общества от электронных коммуникаций и Интернета ведет к тому, что манипуляция социальными сетями позволяет использовать уязвимости национальной и международной безопасности, усиливающиеся вследствие процессов глобальной информатизации.

С развитием информационного общества устаревают традиционные механизмы обеспечения международной безопасности и стабилизации международных отношений, а новые, такие как многоуровневая дипломатия и многосторонние партнерства, пока находятся на начальной или ранней стадиях развития. Основные направления международного сотрудничества по обеспечению международной информационной безопасности рассмотрены в следующей главе настоящего исследования.

ГЛАВА 3. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Формирование международных режимов информационной безопасности на различных уровнях мировой политики

Россия стала первым государством, инициировавшим развитие международного сотрудничества по обеспечению информационной безопасности. Россия выступает за развитие международного сотрудничества по обеспечению информационной безопасности, как на глобальном, так и на региональном уровне, а также в рамках двусторонних отношений. В 1998 г. Россия впервые предложила США подписать на уровне глав государств совместное заявление по проблематике международной информационной безопасности. Данная идея не была полностью реализована на практике, однако обеспокоенность возникающими угрозами в этой сфере нашла отражение в Совместном российско-американском заявлении об общих вызовах безопасности на рубеже XXI века, подписанного президентами России и США по итогам Московского саммита 2 сентября 1998 года[364].

Дальнейшая работа российской дипломатии и международного сообщества в целом по выработке мер, направленных на обеспечение международной безопасности, вплоть до второй половины 2000-х гг. проводилась в основном через механизм Организации Объединенных Наций, как организации, обладающей универсальным членством и легитимностью.

В силу того, что международная информационная безопасность является секьюритизированной областью и ставки участников переговорного процесса высоки на глобальном уровне достичь консенсуса не удалось. В соответствии с подходом О. Янга к формированию международных режимов, в настоящем

[364] Крутских А.В. К политико-правовым основаниям международной информационной безопасности // Международные процессы. 2007. № 1 (13). URL:http://www.intertrends.ru/thirteen/003.htm

исследовании выделяется три этапа формирования международного режима информационной безопасности: определение повестки дня, переговорная стадия, стадия имплементации достигнутых соглашений. Как отмечает Дж. Фирон, если предмет сотрудничества для акторов представляет значительный интерес, то переговоры как «война на истощение» будут длиться довольно долго и к фазе реализации акторы могут и не перейти. Иными словами, чем выше значимость обсуждаемого вопросов для акторов, тем меньше вероятность заключения работающей договоренности.

Опираясь на теорию секьюритизации, выделяющую три стадии секьюритизации референтных объектов безопасности в восприятии ключевых акторов: неполитизированные, политизированные, секьюризированные, и теорию переговорного торга Дж. Фирона ниже будут проанализированы международные договоренности, достигнутые в рамках международных организаций, на двустороннем уровне и в рамках транснационального взаимодействия негосударственных акторов мировой политики.

3.1.1. Глобальный уровень

3.1.1.1. Организация Объединенных Наций

В рамках ООН обсуждаются различные аспекты проблематики международной информационной безопасности – военно-политические и разоруженческие аспекты, сотрудничество правоохранительных органов государств в противодействии киберпреступности, управление Интернетом. Наиболее политизированной темой, которая оказывает влияние на все другие обсуждаемые проблемы, затрагивающие вопросы развития глобального информационного общества, является проблема военно-политического использования ИКТ (в широком смысле, включая социо-гуманитарные аспекты проблематики).

Инициатором обсуждения проблематики международной информационной безопасности в рамках ООН стала Российская Федерация. Российская сторона в 1998 г. предложила проект резолюции ГА ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», после обсуждения пересмотренный текст резолюции был одобрен консенсусом ГА ООН.

Как описывает А.В. Федоров, в резолюции «была подчеркнута потенциальная, но серьезная опасность использования достижений в информационной сфере в целях, не совместимых с задачами поддержания мировой стабильности. Речь шла о необходимости соблюдения принципов неприменения силы, невмешательства во внутренние дела, расширения спектра прав и свобод человека. Особый акцент был сделан на необходимости предотвратить появление конфронтации в информационной области, способной спровоцировать новый виток гонки вооружений в мире. В этой связи отмечалось, что речь идет о создании информационного оружия и опасности возникновения информационных войн»[365]. В ходе заседания ГА ООН в 1998 г. несколько пересмотренный вариант проекта был одобрен комитетом и принят без голосования (консенсусом) Генеральной Ассамблеей ООН (A/RES/53/70)[366].

Впоследствии резолюции по международной информационной безопасности консенсусом принимались Генассамблеей ООН ежегодно, при этом они развивались и дополнялись, отражая стремительный темп развития ИКТ. По инициативе России в принятой в 1999 г. резолюции ГА ООН № 54/49 впервые была сформулирована «триада угроз» в сфере международной информационной безопасности: применение ИКТ в военных, террористических и преступных целях.

В 2004 г. была создана специальная группа правительственных экспертов для изучения проблемы МИБ. В мандат группы вошло рассмотрение угроз в сфере информационной безопасности, возможных совместных мер по их

[365] Федоров А.В. Информационная безопасность в мировом политическом процессе: учеб. Пособие. М.: МГИМО(У), 2006. - С. 109.
[366] Там же. С. 191.

устранению, а также проведение исследования концепций укрепления безопасности глобальных информационных и телекоммуникационных систем[367]. В состав первой группы правительственны экспертов (ГПЭ) вошли 15 государств. Крутских А.В., российский дипломат, был избран председателем группы, что свидетельствовало о признании инициативной роли Российской Федерации. По итогам работы группы решений принять не удалось: был принят формальный документ, в котором было признано наличие разногласий – то есть, «стороны согласились, что их мнения расходятся».

В 2010 г. на 65-й сессии ГА ООН Первым комитетом консенсусом был принят обновленный российский проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Число соавторов проекта возросло до 36 государств, в том числе включает все государства - члены ОДКБ, ШОС, БРИКС и другие страны, что числе США, Японию, Германию и Канаду. Данная резолюция подтвердила решение о повторном созыве Группы правительственных экспертов, с тем чтобы продолжить исследование угроз в сфере информационной безопасности и возможных совместных мер по их устранению[368]. В результате работы группы был принят итоговый документ, в котором нашли отражение следующие рекомендации по снижению угроз международной информационной безопасности:

- Необходимость межгосударственного диалога по вопросам использования ИКТ государствами в целях снижения рисков и защиты критических информационных инфраструктур;
- Выработка мер доверия и снижения рисков, в том числе обсуждения вопросов использования ИКТ в конфликтах;
- Обмен информацией по национальным стратегиям использования ИКТ, правовому регулированию этой сферы, а также национальным стратегиям обеспечения безопасности в сфере ИКТ;

[367]Там же.
[368]Там же.

- Создание инфраструктуры в наименее развитых странах;
- Разработка терминологии в области информационной безопасности[369].

Группа вновь была созвана в 2014 году, в августе 2015 года прошло ее завершающее заседание. Группа включала в себя экспертов из 20 государств, в том числе включая Россию, США, Китай, Великобританию, Францию, Бразилию, Японию, Южную Корею и Израиль. В результате работы группы был принят итоговый доклад, в котором зафиксированы нормы поведения государств в информационном пространстве, основанные на признании необходимости «поощрять использование ИКТ в мирных целях и предотвращать конфликты, возникающие в результате их применения», в частности, отказ от осуществления кибер-атак на критические информационные инфраструктуры, отказ от внедрения незадекларированных программ в программное обеспечение и другую ИТ-продукцию («закладки»), предотвращение использовании государственной территории и национального сегмента информационного пространства для осуществления кибератак на другие государства[370]. Данный документ не носит обязательного характера, но свидетельствует о том, что государства обозначили возможные рамки переговорного пространства для достижения договоренностей на глобальном уровне в будущем.

В 2017 году завершила свою работу Группа правительственных экспертов ООН по международной информационной безопасности очередного созыва. В роли председателя выступала Германия. Принять консесусный доклад Группе не удалось, что обусловлено обострением противоречий по вопросам того, как должно быть устроено глобальное информационное пространство и на основе каких принципов необходимо осуществлять его регулирование. Россия «продвигала в ходе дискуссии на ГПЭ идею о необходимости предотвращения конфликтов в цифровой сфере, ее демилитаризации, закрепления в ней принципов неприменения силы, уважения государственного суверенитета, невмешательства

[369] Fact Sheet Developments in the Field of Information and Telecommunications in the Context of International Security. UNODA. June, 2013. URL: http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf

[370] Черненко Е. Государствам загрузили мирную программу // Коммерсант. 17.08.2015. URL: http://www.kommersant.ru/doc/2790215

во внутренние дела других государств, соблюдения основных прав и свобод человека»[371].

Принятие доклада свидетельствует о поддержке международным сообществом российской позиции. Россия уже в течение длительного времени выступала в поддержку принятия норм ответственного поведения государств в информационном пространстве. Так, в 2011 г. Россия, Китай, Таджикистан и Узбекистан представили на сессии Генассамблеи ООН совместный проект «Правила поведения в области обеспечения международной информационной безопасности». Авторы документа призвали бороться «с распространением информации, которая вдохновляет терроризм, сепаратизм, экстремизм или подрывает политическую, экономическую и социальную стабильность других стран»[372]. Двумя неделями позже в Екатеринбурге главам силовых ведомств 52 стран был предложен разработанный Совбезом и МИД России проект конвенции ООН «Об обеспечении международной информационной безопасности», в котором детально прописаны нормы регулирования Интернета и обеспечения международной информационной безопасности, основанные на «триаде угроз» МИД: военно-политической, террористической и преступной[373].Среди основных угроз перечислены «использование информационных технологий для враждебных действий и актов агрессии», «подрыв политической, экономической и социальной систем» одного государства другим, «манипулирование потоками в информационном пространстве других государств с целью искажения психологической и духовной среды общества»., а также «массированная психологическая обработка населения для дестабилизации общества и

---

[371] Ответ спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских на вопрос информагентства ТАСС о состоянии международного диалога в этой сфере // Официальный сайт МИД России. 29.06.2017. URL: http://www.mid.ru/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/2804288

[372] Правила поведения в области обеспечения международной информационной безопасности: письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 г. на имя Генерального секретаря. A/66/359.

[373] Конвенция об обеспечении международной информационной безопасности (концепция). Утверждена 22.09.2011. URL:http://mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument

государства»[374]. В 2015 году проект Правил, по содержанию схожий с редакцией 2011 г., вновь был отправлен на рассмотрение Генеральному секретарю ООН.

ООН занимается также более узкими аспектами проблематики, в частности неоднократно принимались резолюции ГА ООН в отношении выработки глобальных стандартов защиты критических информационных инфраструктур. Резолюция "Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур"[375], которая принималась ГА ООН в 2002 (A/RES/57/239), 2003 (A/RES/58/199) и 2009 (A/RES/64/211) гг. Данная резолюция представляет собой добровольный инструмент по оценке национальных усилий в области защиты критических информационных инфраструктур и включает в себя перечень критериев эффективности подобной деятельности.

Важным направлением деятельности ООН также является противодействие киберпреступности. В 2010 г. прошел Конгресс ООН по предупреждению преступности и уголовному правосудию в Сальвадоре, по итогам которого была создана межправительственная группа экспертов ООН открытого состава для исследования проблематики киберпреступности. В результате работы группы был принят доклад, в котором представлен обзор существующих проблем, связанных с пресечением и раскрытием киберпреступлений, обзор лучших практик, а также призыв к развитию международного сотрудничества в данной области на глобальном уровне. В докладе отмечается ,что «возникает риск образования страновых группировок, в рамках которых существуют необходимые полномочия и процедуры для сотрудничества между входящими в их состав странами, но которые по отношению ко всем другим странам ограничиваются "традиционными" видами международного сотрудничества, не учитывающими особенности электронных доказательств и глобальный характер

[374] Там же.
[375] Создание глобальной культуры кибер безопасности и оценка национальных усилий по защите важнейших информационных инфраструктур // Резолюция, принятая Генеральной Ассамблеей 21 декабря 2009 года. A/RES/64/211. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/474/51/PDF/N0947451.pdf?OpenElement

киберпреступности»[376]. Данное утверждение можно распространить и на другие области, связанные с обеспечением информационной и кибербезопасности.

Будучи организацией с универсальным членством и неоспоримой легитимностью ООН является центральной переговорной площадкой, на которой обсуждаются проблемы обеспечения международной информационной безопасности. Вместе с тем, расхождения в позициях государств ведут к тому, что большая часть документов, принятых в рамках ООН, носит рекомендательный характер.

3.1.1.2. Международный Союз Электросвязи

Международный Союз Электросвязи (МСЭ) – специализированная организация «семьи» ООН в области информационно-коммуникационных технологий. Таким образом, проблемы информационной безопасности входят в сферу компетенции МСЭ, однако организация вплоть до 2006 г. не занималась данной проблематикой, что было связано с политизацией данной темы и противоречиями в позициях государств.

Одним из первых документов МСЭ, затрагивающих проблематику МИБ, стал Стратегический план МСЭ на 2008 – 2011 гг., принятый на Полномочной конференции МСЭ в Анталии в 2006 г., который отмечал необходимость эффективного противодействия вызовам и угрозам, возникающим в связи с использованием ИКТ в целях несовместимых с международным миром и безопасностью.

Наиболее значимая инициатива МСЭ в данной области - Международное многостороннее партнерство против киберугроз (IMPACT). В качестве первого в мире всестороннего альянса против киберугроз, поддерживаемого ООН, IMPACT объединяет правительства, академические организации и экспертов отрасли в

[376] Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора. Группа экспертов для проведения всестороннего исследования киберпреступности Вена, 25-28 февраля 2013 года. UNODC/CCPCJ/EG.4/2013/2 URL: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf

целях повышения способности глобального сообщества решать проблемы, связанные с информационной безопасностью. Функции IMPACT включают в себя раннее обнаружение и оповещение о киберугрозах, совместные расследования случаев применения кибероружия, консультации и экспертная помощь пострадавшим государствам. Таким образом, МСЭ, будучи узкоспециализированной организацией, долгое время занимался исключительно технологическими аспектами развития ИКТ, в отношении которых интересы большинства акторов совпадали, однако в виду возрастающей значимости проблемы информационной безопасности дискуссии начали приобретать более политизированный и, следовательно, более конфликтный характер.

В декабре 2012 года в Дубае прошла Всемирная конференция по международной электросвязи, целью которой был пересмотр принятого в 1988 г. Регламента международной электросвязи. На конференции обсуждались вопросы интернационализации управления Интернетом, а также некоторые аспекты проблематики информационной безопасности - предотвращения мошенничества, злоупотребления системой телефонной нумерации и др. Итогом конференции стало подписание заключительных актов Всемирной конференции по международной электросвязи и принятие нового регламента международной электросвязи большинством участников; при этом впервые за всю историю МСЭ итоговый документ не был принят консенсусом (55 стран отказались подписывать итоговый документ). Россия, Китай, ряд арабских государств и страны Центральной Азии поддержали итоговый документ, в то время как США, страны ЕС и ряд других государств отказались от его подписания.

Это дало повод аналитикам говорить о начале «Холодной войны 2.0» понимаемой как противостояние между двумя группами государств – выступающими за открытый и общедоступный (пусть и менее безопасный) Интернет и другой — поддерживающей введение «цифрового суверенитета» в целях обеспечения информационной безопасности[377].

[377] Klimburg A. The Internet Yalta: Commentary // Center for New American Security. 5.02.2013. URL:http://www.cnas.org/theinternetyalta

МСЭ становится все более влиятельной организацией в сфере международной информационной безопасности, несмотря на то, что в сфере ее компетенции находятся, прежде всего, технические вопросы. Данная организация ориентирована на многоуровневое взаимодействие и вовлечение в обсуждение государств и негосударственных акторов.

3.1.1.3. Всемирная встреча на высшем уровне по вопросам развития информационного общества

Проблематика международной информационной безопасности обсуждалась на Всемирной встрече на высшем уровне по вопросам информационного общества (ВВУИО). Первый этап этой встречи проходил в декабре 2003 г. в Женеве, второй – в ноябре 2005 г. в Тунисе.

Участники ВВУИО, проходившей под эгидой МСЭ, внесли вклад в реализацию усилий ООН по обеспечению международной безопасности. По итогам каждого из этапов Встречи в Женеве и Тунисе были приняты два документа «План действий» и «Декларация принципов».

В качестве мер укрепления доверия и безопасности при использовании ИКТ авторы Женевского «Плана действий» выделяли: (1) содействие сотрудничеству в рамках ООН в целях анализа реальных и потенциальных угроз в области ИКТ, (2) решение вопросов безопасности сетей, (3) изучение проблем совершенствованная законодательства, (4) проведение эффективных расследований и пресечение случаев ненадлежащего использования ИКТ[378]. В документах также говорилось о взаимопомощи в сфере профилактики компьютерных инцидентов, поощрении участия в деятельности ООН по укреплению доверия при использовании ИКТ. Состоявшийся в Тунисе в ноябре 2005 г. второй этап Всемирной встречи на

[378]Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/5-R. План действий. — 12 декабря 2003 года.
URL: http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-R.pdf

высшем уровне по вопросам информационного общества в целом подтвердил положения принятых в ходе Женевского этапа встречи документов[379].

К отмечает российский эксперт А.В. Крутских, «в итоговые документы саммита был включен предложенный Россией пункт о том, что ИКТ являются эффективным инструментом содействия делу мира, безопасности и стабильности. В документах также говорилось о недопущении злоупотреблений информационными ресурсами и технологиями. Помимо этого в них подтверждалась необходимость общего понимания участниками целей построения глобального информационного общества. В итоговых документах второго этапа ВВУИО были отражены положения, подтверждающие значимость международного права, национального законодательства и суверенитета»[380].

ВВУИО стала важным шагом в начале процесса интернационализации управления Интернетом при обеспечении стабильности, безопасности и непрерывности функционирования Глобальной сети.

3.1.1.4. ЮНЕСКО

ЮНЕСКО является крупнейшей гуманитарной международной организацией, в сферу компетенции которой входят, среди прочего, правочеловеческие аспекты международной информационной безопасности. Прежде всего, ЮНЕСКО занимается такими вопросами как доступность информации, защита персональных данных, формирования общества знания.

В 1990 г. в ЮНЕСКО был создан Сектор коммуникации и информации, в задачи которого входило изучение современных проблем информационного

---

[379] Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/5-R. План действий. — 12 декабря 2003 года. URL: http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-R.pdf; Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/7-R. Тунисское обязательство. — 18 ноября 2005 года.
URL: http://www.itu.int/wsis/docs2/tunis/off/7-ru.pdf; Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R. Тунисская программа для информационного общества. — 18 ноября 2005 года. URL: http://www.itu.int/wsis/docs2/tunis/off/6rev1-ru.pdf; Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/4-R. Декларация принципов.

[380] Крутских А.В. К политико-правовым основаниям международной информационной безопасности // Международные процессы. 2007. № 1 (13). URL:http://www.intertrends.ru/thirteen/003.htm

общества через призму образования, науки и культуры. Сегодня сфера компетенции Сектора расширилась, и в условиях нарастающей конфронтации в информационном пространстве, она включает в себя такие вопросы, как защита персональных данных в кибер-пространстве, доступность и свобода доступа к информации, недопустимость манипуляции информации. По сути, ЮНЕСКО как международная организация обладает потенциалом этического регулирования использования кибер- и информационного оружия.

Вместе с тем, данная организация в области международной информационной безопасности сталкивается с теми же проблемами, что и другие организации семьи ООН – а именно, расхождениями в интересах различных групп государств, что препятствует достижению консенсуса. Однако преимуществом ЮНЕСКО как справедливо отмечает Н. Хаустов, второй секретарь МИД России, «является тот факт, что в отличие от других организаций, она ориентирована не на политическое обсуждение, а на научное исследование современных вызовов и угроз, … аккумулирует передовые знания лучших ученых мира и формирует рекомендации», что открывает возможность для выработки «мягкого консенсуса» на глобальном уровне в рамках данной организации[381].

3.1.1.5. МАГАТЭ

Среди всех вызовов безопасности, с которыми сталкиваются критические информационные инфраструктуры, наибольшую угрозу представляют вызовы информационным системам, обеспечивающим работу гражданских ядерных объектов. МАГАТЭ, будучи ключевой структурой ООН, обеспечивающей мирный характер использования ядерных технологий, является на сегодняшний

[381] Хаустов Н. Информационная безопасность. Взгляд ЮНЕСКО // Международная жизнь. 2015. № 5. URL: http://www.int.mid.ru/bdomp/mg.nsf/77e721b65d04d47d432567230042cfd9/5e84e9647e6714f143257e530041f05c!OpenDocument

день ведущей международной организацией, занимающейся вопросами информационной безопасности мирного атома[382].

Агентство оказывает консультационные услуги, обучает инспекторов в области компьютерной безопасности, а также оказывает в помощь в организации учений в области компьютерной безопасности как составной части программы ядерной безопасности. В фокусе внимания МАГАТЭ находятся вопросы компьютерной и информационной безопасности и защиты компьютерных информационных систем в рамках режима ядерной безопасности[383]. Первые инициативы МАГАТЭ по информационной безопасности ядерных объектов были запущены в 2012 году в свете атак вируса Stuxnet на ядерные объекты Ирана (АСУП АЭС в Бушере). В 2013 году была инициирована Программа компьютерной и информационной безопасности при Управлении ядерной безопасности МАГАТЭ. Программа включает шесть направлений деятельности– разработку технических руководств, организацию и поддержку форумов по обмену технической информацией, региональные тренинговые мероприятия, региональную и международную экспертную поддержку, предметную экспертизу по реагированию на инциденты, а также деятельность по повышению информационного охвата[384].

Деятельность МАГАТЭ в данной области носит в основном просветительский и информационный характер, организация служит площадкой для обмена опытом. Как отмечают эксперты ПИР-центра, в отсутствии норм и трансграничных инструментов сотрудничества усилия МАГАТЭ по повышению осведомленности и наращиванию потенциала реагирования носят особую ценность, однако для более эффективной борьбы с угрозами информационной безопасности агентству имело бы смысл подтолкнуть государства-члены и международное сообщество к диалогу по поводу формирования более практико-

[382] Компьютерная безопасность на ядерных установках. Справочное руководство. // Серия изданий МАГАТЭ по физической ядерной безопасности № 17. Технические руководящие материалы. МАГАТЭ, Вена, 2012. URL: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527r_web.pdf

[383] IAEA. Computer and information security. // IAEA Official site. URL: https://www.iaea.org/topics/computer-and-information-security

[384] Кибербезопасность гражданских ядерных объектов: оценка угрозы и пути ее преодоления. Доклад ПИР-центра. // Индекс безопасности. 2016. № 3-4. С. 70.

ориентированных механизмов и форматов трансграничного сотрудничества в данной сфере[385].

3.1.1.6. Группа семи

Окинавская хартия глобального информационного общества, принятая на саммите Группы семи в Окинаве, Япония в 2000 г. стала знаковым документом с позиций развития глобального информационного общества, в том числе и в контексте его безопасного развития. В Окинавской хартии было отмечено, что ИКТ являются основным фактором, формирующим общество XXI века, при этом страны признали готовность содействовать переходу к информационному обществу, преодолению «цифрового разрыва».

Данный документ затрагивает вопросы международной безопасности, в частности, в нем отмечена необходимость решения проблем, связанных с обеспечением безопасности использования ИКТ[386]. Как отмечает А.В. Крутских, документ предусматривал сотрудничество государств и негосударственных акторов, в частности, в целях защиты критических информационных инфраструктур было решено привлекать представителей промышленности и негосударственных организаций, поскольку исключительно правительства не способны обеспечить безопасность киберпространства. Страны Группы семи пошли на закрепление в итоговом документе лишь вопросов целостности информационных сетей и пресечения преступлений в компьютерной сфере, обойдя военно-политическую составляющую МИБ. Проблема военного применения ИКТ государствами не была отражена в документе, что стало следствием разногласий между развитыми и развивающимися странами по вопросу информационной безопасности[387]. Таким образом, Окинавская хартия

---

[385] Там же.
[386] Окинавская Хартия глобального информационного общества. Группа восьми. Окинава, 2000. URL: http://www.ifap.ru/ofdocs/okinhar.htm
[387] Крутских А.В. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. – 2007. – № 1(5). – С.28-37. URL:http://www.intertrends.ru/thirteen/003.htm

глобального информационного общества в большей степени отражает позицию развитых стран по вопросам построения общемировой информационной сферы.

Последующие саммиты Группы семи не затрагивали проблематику информационной безопасности, за исключением саммита во Франции в Довиле в 2011 г., получившего название «Электронной восьмерки», где ключевой темой стало развитие Интернета, прежде всего, в области электронной коммерции. Итоговая декларация саммита в Довиле 2011 г. среди прочего содержала указание на потенциальную возможность использования Интернета в целях, противоречащих задачам поддержания международного мира и стабильности или способных оказать негативное воздействие на целостность критически важных систем. Лидеры подчеркнули необходимость международного сотрудничества в многоуровневом формате (с привлечением государств, частного бизнеса, гражданского общества и академического сообщества) для предотвращения преступности и терроризма в сфере ИКТ[388]. Была также отмечена важность международного взаимодействия в целях выработки норм поведения в киберпространстве. Военно-политическая проблематика также не нашла отражения в итоговом документе встречи.

3.1.2. Региональный уровень

3.1.2.1. Шанхайская организация сотрудничества

Специальное заявление о международной информационной безопасности 2006 г. стало первым документом в рамках ШОС, в котором была выражена озабоченность возможным использованием ИКТ в целях, способных нанести ущерб безопасности государства, общества и человека в нарушение основополагающих принципов равноправия и взаимного уважения, невмешательства во внутренние дела, мирного урегулирования конфликтов, неприменения силы.В этой связи было принято решение о создании Группы

[388] Довильская декларация «Группы семи»: «Неизменная приверженность свободе и демократии». Довиль, 2011. URL: http://kremlin.ru/supplement/946

экспертов государств ШОС по МИБ 2006.Результатом дальнейшего углубления международного сотрудничества по МИБ в рамках ШОС стало подписание в 2009 г. Соглашение государств ШОС по МИБ (вступило в силу 2011 г.). Соглашение содержит определение терминов и понятий в области МИБ, характеристику основных угроз в сфере МИБ, основные направления сотрудничества[389].

Целью Соглашения является создание политико-правовых и организационных основ дальнейшего углубления доверия и развития взаимодействия в области международной информационной безопасности. Соглашение определяет наличие и существо конкретных угроз в области МИБ, а также основные направления, принципы, формы и механизмы сотрудничества стороны в этой сфере. Соглашение открыто для присоединения других государств[390].

В январе 2015 г. государствами-членами ШОС внесены в качестве официального документа ООН «Правила поведения в области обеспечения международной информационной безопасности (МИБ)». Документ опирается на подходы, заложенные в проекте «Правил поведения в области обеспечения МИБ», распространенном от имени государств-членов ШОС в ходе 66-й сессии Генеральной Ассамблеи ООН в 2011 г. В новой редакции «Правил поведения» идеи были преобразованы с учетом изменившихся реалий и предложений, поступивших от заинтересованных государств. Документ нацелен на предотвращение конфликтов в информационном пространстве. В Правила включен расширенный правочеловеческий раздел, указано, что права, которые человек имеет в офф-лайновой среде, должны также защищаться в онлайновой среде, при этом пользование данными правами может быть сопряжено с некоторыми ограничениями в соответствии со ст.19 Международного пакта о гражданских и политических правах. Вопросы интернационализации управления Интернетом вынесены в документе в качестве отдельного пункта. Особое

---

[389] Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2009 г.

[390]Глобальная безопасность: инновационные методы анализа конфликтов / под общ. ред. А.И. Смирнова. М.: Общество «Знание» России, 2011. С. 185.

внимание уделяется также проблематике «наращивания потенциала» в сфере информационной безопасности и оказания развивающимся странам содействия в преодолении «цифрового разрыва»[391].

Таким образом, сотрудничество по вопросам МИБ на площадке ШОС успешно развивается, что связано, прежде всего, с общим пониманием угроз информационной безопасности и подходов к ее обеспечению. Все государства-участники ШОС привержены расширительной трактовке безопасности в цифровой среде, включая в нее социо-гуманитарные аспекты использования ИКТ, а также идее «цифрового суверенитета» и интернационализации управления Интернетом. Вместе с тем, сотрудничество в рамках ШОС в данной области носит политический характер и не затрагивает экономические аспекты использования ИКТ.

3.1.2.2. Содружество независимых государств

Первоначально деятельность СНГ в области МИБ ограничивалась гармонизацией законодательства и работой над терминологией и понятийным аппаратом. Впервые термин «информационная безопасность» появляется в документах СНГ в конце 1990-х гг. Модельный закон СНГ «О международном информационном обмене»[5] раскрывает это понятие: «Информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства».Впоследствии в рамках СНГ также началась работа по гармонизации правового пространства СНГ и разрабатываются модельные законы, направленные на регулирование Интернета и иных ИКТ[392]. По оценкам экспертов, государства-члены СНГ недостаточно активно используют

[391]Сообщение для СМИ. Об инициативе стран-членов ШОС «Правила поведения в области обеспечения международной информационной безопасности» // МИД России. Официальный сайт. 29.01.2015. URL: http://www.mid.ru/brp_4.nsf/newsline/BA8A7E45ED6164CA43257DDC0050C89E

[392] Об Интернете: проект модельного закона СНГ // Межпарламентская ассамблея государств - участников СНГ, 2007. URL:http://www.raecs.ru/files/modelnyi_zakon_sng_po_intrnetu.pdf; Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. Минск, 2001. URL:http://www.gipi.kg/rus/readarticle.php?article_id=131;

модельное законодательство СНГ в целях национальных модернизации правовых систем и развития информационного права[393].

В рамках СНГ было заключено Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 2001 г. и Соглашение о сотрудничестве в реализации и формировании информационных ресурсов и систем от 1999 г[394].

Комиссия по информационной безопасности была создана по решению Координационного совета государств - участников СНГ по информатизации при Региональном содружестве связи (РСС) в декабре 2004 года, в 2011 году была преобразована Комиссию РСС по информационной безопасности. С участием членов Комиссии РСС по информационной безопасности подготовлены и приняты высшими органами СНГ ряд документов, способствующих созданию организационно-правовых основ сотрудничества в сфере обеспечения информационной безопасности в государствах-участниках СНГ:

- Стратегия сотрудничества государств-участников СНГ в сфере информатизации и Плана действий по ее реализации до 2010 года, в части информационной безопасности
- Концепция сотрудничества государств-участников СНГ сфере обеспечения информационной безопасности и Комплексного плана мероприятий по ее реализации до 2010 года
- Стратегия сотрудничества государств-участников СНГ в построении и развитии информационного общества и Плана действий до 2015 года, в части информационной безопасности.
- Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности[395].

---

[393] В Госдуме забраковали проект модельного закона СНГ "О праве собственности и его защите" из-за нового ГК РФ // Право.ру. 02.07.2011. URL: http://pravo.ru/news/view/55088/

[394]Итоговый документ Международного семинара «Управление использованием Интернета». Кишинев, 2005. URL:http://www.rcc.org.ru/ru/news/documents/2005-01.doc

[395] Комиссия РСС по информационной безопасности // Региональное содружество в области связи. Официальный сайт. URL: http://www.rcc.org.ru/index.php?option=com_content&view=section&id=39&Itemid=549

В ходе саммита в Минске в ноябре 2014 г. государства - участники СНГ выразили готовность поддержать инициативу о создании единого Центра обеспечения безопасности киберпространства СНГ (CERT - Computer Emergency Response Team).

Несмотря на то, что инициативы СНГ в российских СМИ привлекают к себе меньшее внимание по сравнению с ШОС, они выполняют важные функции выстраивания единого правового пространства в сфере ИКТ, а также решения важных технических аспектов с сфере общей кибербезопасности (сотрудничество на уровне CERT). Вместе с тем, разнородность государств участников СНГ и различия в подходах к обеспечению безопасности, а также в уровнях развития информационного общества и природе угроз, с которыми страны сталкиваются, ведет к тому, что политическая проблематика МИБ в рамках данной организации не обсуждается, то есть на практике происходит реализация «сотрудничества на разных скоростях», когда центр тяжести военно-политического сотрудничества переносится на уровень ОДКБ.

3.1.2.5. Организация договора коллективной безопасности

Сотрудничество на этом направлении реализуется в соответствии с Программой совместных действий по формированию системы информационной безопасности государств-членов ОДКБ, утвержденной Советом коллективной безопасности Организации в сентябре 2008 года. Программа охватывает такие направления, как сотрудничество в политической сфере, совместные научные и исследовательские разработки и обмен информацией о достижениях в этой области, подготовка кадров, унификация законодательной и нормативно-правовой базы, совместное обеспечение безопасности жизненно важных объектов, проведение совместных мероприятий, направленных на борьбу с преступлениями в сфере ИКТ[396].

[396]Кожевников А.В. О коллективных мерах государств - членов ОДКБ в сфере обеспечения информационной безопасности // Международный терроризм в информационную эпоху: реалии кибертерроризма и кибероружия,

Правовая база сотрудничества определяется Положением о сотрудничестве в сфере информационной безопасности государств-членов ОДКБ.Взаимодействие ведется также на уровне специальных подразделений органов безопасности и внутренних дел (полиции) в целях противодействия преступлениям в сфере современных информационных технологий в рамках операции «ПРОКСИ»[397].

Таким образом, ОДКБ, будучи организацией коллективной безопасности, переносит свои функции в информационную сферу, которая в современных условиях трактуется как источник вызовов национальной и международной безопасности, причем в рамках ОДКБ удалось договориться о мерах доверия и иных формах международного сотрудничества, что об общности интересов государств и подходов к обеспечению информационной безопасности.

3.1.2.3. Организация по безопасности и сотрудничеству в Европе

Впервые вопросы сотрудничества в сфере международной информационной безопасности обсуждались в ходе Межпарламентской ассамблеи стран Организации по безопасности и сотрудничеству в Европе (ОБСЕ) в Санкт-Петербурге в 2008 году. В марте 2009 г. прошло Рабочее совещание ОБСЕ по всеобъемлющему подходу ОБСЕ к повышению кибербезопасности.

В ходе «Конференции ОБСЕ по всеобъемлющему подходу к кибербезопасности: определение будущей роли ОБСЕ» в 2011 г. обсуждалась перспектива выработки правил поведения международного сотрудничества в области информационной безопасности в рамках ОБСЕ. Однако, несмотря на то, что все участники организации признали целесообразность выработки в рамках данной организации кодекса поведения в области международной

терроризм и средства массовой информации: сб. материалов международной конференции. М., 2010. URL:http://catu.su/index.php?option=com_content&view=article&id=155%3A2011-11-18-13-13-16&catid=38%3Aslideshow&Itemid=91

[397] Выступление Генерального секретаря Организации Договора о коллективной безопасности Н.Н. Бордюжи на совместном заседании Постоянного совета ОБСЕ и Форума по сотрудничеству в области безопасности, Вена, 15 апреля 2010 года // МИД России. Официальный сайт. URL: http://www.mid.ru/bdomp/Ns-dos.nsf/44a7dafc231dc11ac32576d6002f70c1/b6baf366e4569788c325771a0046b181!OpenDocument

информационной безопасности, международное сотрудничество в данной области зашло в тупик.

В декабре 2013 г. Постоянный совет ОБСЕ одобрил документ «Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью снижения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий». Разработка данного документа стала возможна благодаря уже достигнутым между США и РФ договорённостям по вопросам укрепления мер доверия в киберпространстве[398]. В марте 2016 года ОБСЕ принята «Дополнительный перечень мер укрепления доверия в рамках ОБСЕ с целью снижения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий». Таким образом, ОБСЕ вносит вклад в развитие норм мягкого права в области информационной безопасности, вместе с тем, главным недостатком указанных мер доверия является их добровольный характер и неопределенность

ОБСЕ является, по сути, «малой ООН» для Европы, поэтому ее участие в обеспечении информационной представляется очень перспективным, однако ОБСЕ на данном направлении сталкивается с теми же проблемами, что и ООН – различными подходами государств к определению угроз в безопасности в условиях глобальной информатизации и несовместимыми подходами к ее обеспечению.

3.1.2.4. Совет Европы

Конвенция Совета Европы о киберпреступности 2001 г. (Будапештская конвенция) является на сегодняшний день единственным многосторонним документам, разработанным с целью противодействия угрозам в цифровой среде. Конвенция содержит перечень киберпреступлений и предполагает создание механизмов международного сотрудничества по предотвращению, раскрытию и

[398] Батуева Е.В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая // Дисс. … ученой степени кандидата политических наук. М.: МГИМО, 2015.

преследованию киберпреступлений. Кроме того, в 2006 г. был принят Дополнительный протокола к Конвенции, касающийся уголовной ответственности за акты расистского и ксенофобского характера, совершаемые через компьютерные системы. На сегодняшний день Конвенцию ратифицировали 45 стран. Однако Россия не присоединилась к данной конвенции в виду того, что отдельные ее положения, согласно официальной позиции, нарушают государственный суверенитет. Статья 32 “b” допускает проведение оперативно-розыскной деятельности в информационном пространстве других государств без их уведомления. Согласно официальной позиции России и ряда других государств, ряд положений конвенции, разработанной в 2001 г., устарели в современных условиях. В частности, она криминализирует всего 9 видов незаконного использования ИКТ, а сейчас их уже около 30[399]. Россия выступает за создание под эгидой ООН универсальной конвенции по противодействию преступлениям в информационной сфере, которая должна носить глобальный характер и основываться на фундаментальных принципах международного права, включая суверенное равенство государств и невмешательство во внутренние дела.

В апреле 2015 г. Комитет министров Совета Европы (СЕ) утвердил для всех входящих в него государств рекомендации о принципах регулирования Интернета. Данные правила включают в себя единые правила хранения и распространения информации в электронных сетях, а также контроля за их использованием со стороны властей и работодателей. Борьба властей с незаконным контентом не должна нарушать нормы Европейской конвенции по правам человека, а уже принятые меры по блокировке сайтов следует "регулярно пересматривать". Меры направлены, прежде всего, на защиту детей, частной и семейной жизни, персональных данных и борьбу с киберпреступностью[400].

---

[399] Крутских А.В. Международный политический процесс по нахождению решений в области международной информационной безопасности // Digital Report. 29.04.2015. URL: http://digital.report/mezhdunarodnyiy-politicheskiy-protsess-po-nahozhdeniyu-resheniy-v-oblasti-mezhdunarodnoy-informatsionnoy-bezopasnosti/

[400] Пушканская А. Пусть все идет по трафику // Коммерсант. 04.04.2015. URL: http://www.kommersant.ru/doc/2702084

3.1.2.6. Европейский союз

На уровне Европейского союза рассматриваются в основном экономические проблемы сотрудничества по обеспечению кибербезопасности, военно-политическая политическая составляющая входит в компетенцию НАТО. Вместе с тем, в последние годы ЕС выступает с предложениями расширить взаимодействие с НАТО в сфере кибербезопасности и перенести ряд функций в этой области на уровень ЕС. Это связано с тем, что после вступления в силу Лиссабонского договора проблематика кибербезопасности рассматривается как одно из направлений ОВПБ ЕС. Вместе с тем, на уровне ЕС не было создано единого органа, отвечающего за сотрудничество в сфере кибербезопасности.

2013 г. была принята Стратегия ЕС обеспечения безопасности киберпространства. В стратегии, в частности, определены 5 приоритетов: достижение кибер-жизнестойкости, значительное сокращение кибер-преступности, развитие политики кибер-защиты, развитие промышленных и технологических ресурсов для кибер-безопасности, создание гармоничной международной политики в сфере кибер-пространства[401]. В рамках этой инициативы Агентство ЕС по безопасности сетей и информации (ENISA) организовывает учения стран ЕС по проверке готовности к отражению кибератак. Последнее такое учение прошло в 2014 году. Кроме того, в рамках ENISA было разработано специальное руководство (Good Practice Guide), затрагивающее безопасность критических информационных инфраструктур. В руководстве даются рекомендации, а также передовая практика по разработке, внедрению и поддержке в актуальном состоянии стратегии кибербезопасности[402].

Евросоюз также ввел правила защиты персональных данных граждан. Директива по сетевой информационной безопасности обязывает 27 государств-членов ЕС улучшить уровень подготовленности для противостояния хакерским

[401] Cyber Security strategy of the European Union: An open, safe and secure Cyberspace. JOIN (2013). European Commission. Brussels, 7.02.2013. URL: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[402] Cybersecurity. Digital Agenda for Europe. A Europe 2020 Initiative // European Commission. Official site. URL: https://ec.europa.eu/digital-agenda/en/cybersecurity

атакам путем создания групп экстренного реагирования для борьбы с кибератаками[403].

Кроме того, в 2016 году была принята Директива Европейского парламента о безопасности компьютерных сетей и информационных систем, в соответствии с которой компании, работающие в странах ЕС в энергетической, транспортной, нефтегазовой, медицинской, финансовой и других сферах (то есть оперирующие критическими информационными инфраструктурами), проходят обязательное тестирование информационной безопасности. Компании также обязаны информировать государства ЕС о сбоях в защите информационных систем. Особое внимание уделяется безопасности финансовых площадок в интернете, облачных хранилищ и поисковых систем, как наиболее уязвимых с точки зрения киберугроз. В соответствии с директивой страны-члены ЕС должны также создать группы реагирования на инциденты, связанные с кибербезопасностью (CSIRT), которые впоследствии будут объединены в единую сеть. Государства также должны будут создать ведомства в области информационной безопасности при правительстве, разработать национальные стратегии информационной безопасности. На общеевропейском уровне будет создана специальная Группа кооперации, при посредничестве которой страны-участницы будут делиться информацией об инцидентах и угрозах[404].

Таким образом, интенсифицируется сотрудничество в области информационной безопасности на общеевропейском уровне, создавая определенный противовес действиям НАТО в данной области. Кроме того, отчетность и тестирование компаний в сфере информационной безопасности может создать определенные затруднения для работы компаний GAFA (Google-Apple-Facebook-Amazon) на европейских рынках.

---

[403] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. COM (2013) European Commission. Brussels, 7.02.2013 URL: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[404] Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union. 6.07.2016. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

Таким образом, в рамках ЕС кибербезопасность трактуется в рамках защиты критических информационных инфраструктур. Однако большая часть деятельности по обеспечении безопасности критических инфраструктур находится в компетенции государств, каждая из которых принимает национальную стратегию кибербезопасности. ЕС вырабатывает директивы, согласовывающие подходы, и создает механизмы взаимодействия по предотвращению киберугроз или ликвидации их последствий (что необходимо в условиях, когда большая часть критических информационных инфраструктур ЕС не локализована в рамках одного государства).

3.1.2.7. НАТО

В 2008 году по инициативе Эстонии в Таллине был создан центр передового опыта НАТО в области компьютерной безопасности. В настоящее время он является основным научно-исследовательским и учебным заведением альянса, занимающимся разработкой ключевых направлений развития коалиционных возможностей по действиям в киберпространстве, а также эффективных мер информационной защиты объектов военной и гражданской инфраструктуры. Основным результатом экспертной работы центра стала публикация в 2013 г. Таллинского руководства по ведению кибервойн, содержащего 95 правил, регламентирующих применение международного гуманитарного права к конфликтам в цифровой среде[405].

В Стратегической концепции альянса принятой в 2010 г. на саммите в Лиссабоне, определяющей основные вызовы и угрозы, говорится о необходимости создания потенциала для выявления, предотвращения и защиты от кибернетических атак. Для этого требуется задействовать механизмы объединённого планирования, координировать национальные программы защиты киберпространства, включая совместную работу систем предупреждения и реагирования на кибератаки, а также создать единую систему информационной

[405] Tallinn Manual on the International Law Applicable to Cyber Warfare / ed. by M. Schmitt – N.Y.: Cambridge University Press, 2013.

безопасности для всех структур НАТО. Таким образом, в стратегическую концепцию НАТО впервые включено положение о киберпространстве как новой сфере военной деятельности альянса. При этом в экспертных кругах полагают, что компьютерные атаки могут быть приравнены к началу боевых действий[406].

В 2013 году было завершено развертывание единой системы НАТО по реагированию на компьютерные угрозы, которая предназначена для своевременного выявления и нейтрализации киберугроз, а при необходимости и восстановления в работоспособности компьютерных сетей органов управления стран - участниц Североатлантического союза.

Новая политика кибербезопасности НАТО призывает всех членов обмениваться своим опытом в кибербезопасности. Она была одобрена на саммите в сентябре 2014 года, после чего последовали широкомасштабные киберучения для проверки системных уязвимостей инфраструктуры[407].

Однако, остается открытым вопрос о разделении полномочий и сфер деятельности между коалиционными и национальными органами и службами. США и Великобритания выступают за возложение на Североатлантический союз всей полноты ответственности за обеспечение защиты от киберугроз, что приведет к выстраиванию системы коллективной кибероборонына базе американских технологий и максимальном привлечении американских IT-компаний. В то же время наиболее развитые в области кибербезопасности европейские страны (Германия, Франция, Италия и Испания) относят вопросы строительства и управления киберпотенциалом к национальной сфере компетенции, отводя НАТО лишь координирующую роль[408].

При этом НАТО, несмотря на официальную позицию, уделяет внимание не только вопросам кибербезопасности, но и информационного содержания сети. В

---

[406] См. напр.: Градов А. Деятельность североатлантического союза в сфере кибербезопасности (2014) // Зарубежное военное обозрение. 2014, №7, С. 13-16. URL: http://factmil.com/publ/strana/nato/dejatelnost_severoatlanticheskogo_sojuza_v_sfere_kiberbezopasnosti_2014/61-1-0-452

[407] Куликова А. Возможна ли гонка кибервооружений между Россией и США? // ПИР Центр 28.01.2015. URL: http://pircenter.org/media/content/files/13/14243529940.pdf

[408] Градов А. Деятельность североатлантического союза в сфере кибербезопасности (2014) // Зарубежное военное обозрение. 2014, №7, С. 13-16. URL: http://factmil.com/publ/strana/nato/dejatelnost_severoatlanticheskogo_sojuza_v_sfere_kiberbezopasnosti_2014/61-1-0-452

августе 2015 года в Риге, Латвия был открыт созданный более года назад Центр стратегической коммуникации НАТО. Официально миссия центра предполагает оказание поддержки НАТО в стратегической коммуникации[409]. Вместе с тем, реализация подобной миссии предполагает, противодействие информационной политике России. Кроме того, в рамках центра проводится изучение возможности использования «больших данных»[410] в стратегической коммуникации, что представляет собой проблему на стыке информационной и кибербезопасности, потому что технологически «большие данные» могут быть использованы в целях социального инжиниринга и воздействия на общественное мнение, то есть как информационное оружие.

В целом же, можно констатировать признание на уровне НАТО значимости кибер и информационных угроз для национальной и региональной безопасности и стремление задействовать коалиционные механизмы для противодействия и предупреждения, таким образом, формируя военно-политическое взаимодействие по обеспечению кибер и информационной безопасности.

3.1.2.8. АСЕАН

Первым документов в данной области стало Заявление Регионального форума АСЕАН о сотрудничестве по противодействию кибератакам и террористическому использованию киберпространства от 2006 года. В 2010 г. решением 17-й сессии Регионального форума АСЕАН по вопросам безопасности (АРФ) за Россией наряду с Австралией и Малайзией была закреплена курирующая роль в проработке проблематики кибербезопасности и борьбы с кибертерроризмом. В 2012 году было принято заявление Регионального форума о сотрудничества в области кибербезопасности, подготовленное при участии России.

---

[409]NATO Strategic Communications Centre of Excellence Riga, Latvia. Official site. URL: http://www.stratcomcoe.org/Organisation/MissionAndTasks.aspx

[410]Тамже.

На площадке АСЕАН взаимодействие ведется в многоуровневом формате с привлечением бизнеса, гражданского общества и исследовательского сообщества, при этом безопасность трактуется, прежде всего, в ее информационно-техническом измерении (как кибербезопасность).

Сотрудничество ведется по следующим направлениям:

- Ежегодные киберучения
- Взаимодействие в реальном времени
- Исследовательская работа
- управление инцидентами и уязвимостями, расследование
- обмен информацией об угрозах.

Наиболее успешным является сотрудничество на техническом уровне: была создана сеть CERT Asia Pacific Computer Emergency Response Team (APCERT), которая объединяет усилия 30 команд из 20 стран.

Таким образом, сотрудничество в рамках АСЕАН и ЕС по обеспечению кибербезопасности строится по схожей модели – обе интеграционные структуры признают значимость угроз, прежде всего, в контексте защиты критических информационных инфраструктур, однако, принимая во внимание чувствительный характер проблемы, основные политические компетенции в данной сфере сохраняются на национальном уровне. При этом АСЕАН создает условия для взаимодействия по предотвращению киберугроз, обмену информацией и лучшими практиками, а также механизмы взаимодействия между правоохранительными органами государств и иными службами безопасности, участвующими в противодействии киберпреступности и иным видам кибератак. Сотрудничество с АСЕАН позволяет России получить доступ к лучшим практикам, сложившимся в рамках данного региона, а также органично участвовать информационного пространства АСЕАН, участники которого рассматриваются как потенциальные экономические партнеры России в сфере ИТ.

3.1.2.9. АТЭС

На уровне АТЭС знаковым событием в области информационной безопасности стал саммит в России в 2011 г. В ходе подготовки к саммиту на уровне министров связи была принята Петербургская декларация «Укрепление доверия и безопасности при использовании ИКТ в целях содействия экономическому росту и процветанию». Несмотря на то, что проблема информационной безопасности не является приоритетной темой декларации, она упомянута в контексте необходимости создания безопасной электронной среды для экономического развития стран участниц организации. Подобный подход представляется обоснованным, так как организация представляет собой, прежде всего, экономический форум, и проблематика информационной безопасности рассматривается через призму ее экономической составляющей.

АТЭС разработала основные принципы, которыми надлежит руководствоваться при создании и использовании так называемых групп реагирования на компьютерные инциденты (CERTs) для целей раннего предупреждения и защиты от кибернападений.

Отметим, что значимость АТЭС в данной области также обусловлена наличием площадки для взаимодействия бизнес-структур, в том числе и в ИТ-области, что создает основу для продвижения инициатив многоуровневого сотрудничества в области информационной безопасности и в сфере ИКТ в целом.

3.1.2.10. БРИКС

Проблематика информационной безопасности до недавнего времени не обсуждалась на площадке БРИКС. В 2015 году на саммите БРИКС в Бразилии, в г. Форталеза вопросам информационной безопасности было уделено значительное внимание. В декларации зафиксировано стремление к международному сотрудничеству в сфере МИБ на основе «общепризнанных норм и принципов международного права». При этом отмечалась значимость многоуровневого

взаимодействия, при участии государств, бизнеса, гражданского общества и научного сообщества[411].

Главы государств БРИКС осудили «акты массовой электронной слежки и сбора данных о частных лицах по всему миру, а также нарушение суверенитета государств и прав человека, и в частности, права на неприкосновенность частной жизни»[412]. В декларации сказано, что для борьбы с киберпреступностью необходим «универсальный, имеющий обязательную юридическую силу международно-правовой документ»[413]. Особо подчеркнута центральная роль ООН в этом вопросе.

Отдельно было отмечено российское предложение совместно разработать соглашения между странами БРИКС о сотрудничестве по вопросам национальной безопасности. Для этого будет создана группа экспертов из стран БРИКС[414].Согласно официальным заявлениям, на уровне БРИКС проводятся консультации по возможному созданию дублирующей инфраструктуры Интернета[415].

Таким образом, в условиях отсутствия консенсуса на глобальном уровне международное сотрудничество в основном носит исследовательский характер (изучение угроз, а также поиск возможных областей совпадения интересов), также вырабатываются нормы «мягкого права» в области международной информационной безопасности, не носящие обязательного характера, но отражающие позицию и интересы большей части международного сообщества.

Следует также отметить распространение форматов многоуровневого сотрудничества, прежде всего, в рамках ООН, как на политическом уровне, так и в рамках взаимодействия по узкоспециализированной технической проблематике.

---

[411] Форталезская декларация (принята по итогам шестого саммита БРИКС) Форталеза, 15.08. 2014 URL: http://static.kremlin.ru/media/events/files/41d4f1dd6741763252a8.pdf

[412] Там же.

[413] Там же.

[414] Тодоров В. Рунет продублируют по-китайски // Газета.ru 29.10.2014. URL: http://www.gazeta.ru/business/2014/10/29/6281217.shtml

[415]Там же.

3.1.3. Двусторонний уровень

В условиях сложности достижения консенсуса на глобальном уровне, особое значение принимают двусторонние договоренности в сфере информационной или кибербезопасности. На сегодняшний день насчитывается множество подобных соглашений.

В частности, Россией подписаны двусторонние соглашения по сотрудничеству в сфере международной информационной безопасности с Бразилией в 2010 г., республикой Беларусь в 2013 г., США в 2013 г., Кубой в 2014 г. и Китаем в 2015 г. Наиболее значимыми с точки зрения российских интересов являются соглашения с США и Китаем.

Соглашение о мерах доверия с США 2013 г. Соглашение о мерах доверия в киберпространствемежду Россией и США было подписано в июне 2013 года в присутствии Барака Обамы и Владимира Путина. Оно включало в себя три документа, оговаривающих создание между Москвой и Вашингтоном прямых линий связи по предотвращению эскалации киберинцидентов, обмен информацией между кураторами вопросов национальной безопасности и группами экстренной готовности к инцидентам. Развитием сотрудничества должна была заняться специальная рабочая группа, однако Вашингтон приостановил свое участие в рабочей группев результате общего похолодания в отношениях после воссоединения России с Крымом. Однако прямая линия связи продолжает функционировать, что указывает на взаимозависимость и уязвимость сторон, и необходимость поддержания диалога и сохранения доверия в данной области. Сохраняются также контакты России и США по информационной безопасности по линии ГПЭ ООН.В октябре 2016 года впервые была использована прямая линия – президент США связался с Москвой в связи с хакерскими атаками на политические институты США в предверии выборов президента США, в которых США обвиняют Россию[416]. Б. Обама заявил, что в

[416]GRIZZLY STEPPE – Russian Malicious Cyber Activity. Joint Analysis Report. Us Department of Homeland Security, Federal bureau of Investigation. 29.12.2016. URL: https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

случае вмешательства в информационную систему выборов США готовы использовать ответные меры, в том числе вооруженные[417].

В мае 2015 года было подписано двустороннее межправительственное Российско-Китайское соглашение о сотрудничестве в сфере информационной безопасности. В документе отмечаются следующие направления международного сотрудничества в сфере МИБ: обмен информацией между спецслужбами, совместный мониторинг и предотвращении инцидентов и конфликтов в киберпространстве, обеспечение безопасности критических информационных инфраструктур, борьба с информационным терроризмом. Российско-китайское соглашение также выделяет меры доверия в числе основных механизмов сотрудничества. В документе упоминается значимость угроз информационной безопасности с точки зрения стратегической стабильности, что выводит их на новый уровень приоритетности с точки зрения выделяемых ресурсов. В СМИ подписанное соглашение, как и соглашение России и США от 2013 г. получило название «пакта о киберненападении». Действительно, в документе содержится обязательство «невмешательства в информационные ресурсы Сторон»[418].Кроме того, государства договорились о том, что «Каждая Сторона не осуществляет по отношению к другой Стороне» ... «несанкционированное вмешательство и атаки» на информационные ресурсы»[419].В целом, анализ содержания документа и обозначенных в нем основных направлений сотрудничества указывает на то, что данное соглашение может быть классифицировано как соглашение о военно-политическом сотрудничестве в сфере обеспечения информационной безопасности.

Политические шаги между Россией и Китаем в данной области сопровождаются экономическим сотрудничеством. "Ростелеком" совместно с китайской Huawei планирует строительство подводной линии связи Магадан-

[417] Arkin W., Dilanian D. What Obama Said to Putin on the Red Phone About the Election Hack. NBC, 19.12.2016. URL: http://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116

[418] Распоряжение Правительства Российской Федерации О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности. Москва, 30.04.2015. № 788-р. URL: http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf

[419] Там же.

Сахалин-Камчатка, согласно достигнутым договоренностям запланировано также увеличении экспорта российского софта в Китай и о поставках в Россию продукции крупнейшего в Китае производителя серверов Inspur Group[420].

4 сентября 2017 года «на полях» БРИКС было подписано соглашение между Россией и ЮАР о сотрудничестве в области обеспечения международной информационной безопасности. В документе отмечается общее понимание угроз международной информационной безопасности. Кроме того, «данный документ позволяет России и ЮАР более тесно координировать подходы к проблематике МИБ на международной арене, включая такие площадки, как ООН, БРИКС и Международный союз электросвязи»[421]. Помимо этого документ предполагает развитие сотрудничества по следующим направлениям: формирование «истемы совместного реагирования на угрозы в этой сфере, реализации двусторонних мер доверия, сотрудничестве в правоохранительной области для расследования дел, связанных с использованием ИКТ в террористических и других криминальных целях, взаимодействии в разработке и продвижении соответствующих норм международного права, проведении совместных научно-исследовательских работ, подготовке профильных специалистов»[422]. Кроме того, Россия заключила двусторонние соглашения в данной области с Бразилией и Индией[423].

США имеет соглашения о мерах доверия в области кибербезопасности с Индией. Подписанный меморандум о взаимопонимании не носит обязательного характера, ориентирован на развитие технического взаимодействия и предполагает обмен разведданными и передовым опытом в сфере кибербезопасности и координацию работы Групп быстрого реагирования на

---

[420] Братья на web // Коммерсант. 21.10.2014. URL: http://www.kommersant.ru/doc/2594090

[421] О подписании Соглашения между Правительством Российской Федерации и Правительством Южно-Африканской Республики о сотрудничестве в области обеспечения международной информационной безопасности. Сообщение для СМИ. // Официальный сайт МИД России. 4.09.2017. URL: http://www.mid.ru/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/2854430

[422] Там же.

[423] Интервью спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских телеканалу «Раша Тудэй», 24 июля 2017 года // Официальный сайт МИД России. 24.07.2017. URL: http://www.mid.ru/web/guest/nota-bene/-/asset_publisher/dx7DsH1WAM6w/content/id/2822103

киберинциденты (CERT)[424].В целом, в настоящее время внешнеполитическая стратегия США в сфере информационной безопасности ориентирована на включение проблематики кибербезопасности в существующие двусторонние и многосторонние договоренности военно-политического характера, что соотносится с действующей киберстратегией США[425]. В частности, на двустороннем уровне США и Япония обмениваются информацией о киберугрозах и киберинцидентах, причем сотрудничество в данной области в перспективе планируется расширить[426]. 25сентября 2015 г. было достигнуто соглашение между США и КНР о сотрудничестве в области кибербезопасности, что включает в себя своевременный обмен информацией о кибератаках, отказ от взаимного кибершпионажа, взаимодействие в области расследования киберпреступлений и судебного преследования виновных[427].

Европейские страны также задействуют подобный формат сотрудничества, в качестве примера можно привести Кибер диалог Япония – ЕС, направленный против потенциальных киберугроз со стороны Китая[428].

Отметим, что двустороннее взаимодействие является важной составляющей в формировании международного режима информационной безопасности, так как позволяет обеспечить формирование доверия в двусторонних отношениях, снизив риски и угрозы эскалации конфликта, и таким образом, способствуя международной стабильности.

3.1.4. Транснациональный уровень

[424] United States and India Sign Cybersecurity Agreement // USA Department of Homeland Security. Press Release. Washington, 19/07/2011. URL: http://www.dhs.gov/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement

[425]The Department of Defense Cyber Strategy. Washington, April, 2015. URL: http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[426] Gady F. Japan and the United States to Deepen Cybersecurity Cooperation // The Diplomat. 02.06.2015. URL: http://thediplomat.com/2015/06/japan-and-the-united-states-to-deepen-cybersecurity-cooperation/

[427] Fact Sheet: President Xi Jinping's State Visit to the United States. // The White House. Office of the Press Secretary. 25.09.2015. URL: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

[428] Gady F. Japan and Europe Step Up Cooperation in Cyberspace // The Diplomat. 13.01.2015. URL: http://thediplomat.com/2015/01/japan-and-europe-step-up-cooperation-in-cyberspace/

Негосударственные транснациональные акторы (бизнес-структуры, экспертные сообщества и НПО) играют существенную роль в глобальном информационном пространстве, и, как следствие, формируют частные международные режимы, направленные на обеспечение кибербезопасности. Вместе с тем, исключительно частных инициатив в области информационной безопасности на международном уровне не так много, большая часть международных мер носит либо многоуровневый, либо межгосударственный характер.

Так, технические стандарты Интернета, в том числе в области информационной безопасности, разрабатываются и контролируются частной организацией Рабочая группа Интернет-инжиниринга (Internet Engineering Task Force “IETF”). Изначально, данная структура состояла исключительно из американских исследователей, финансировалась правительством США и выполняла правительственные заказы. Сейчас организация допускает участие представителей различных государств, частного бизнеса, исследователей на транснациональной основе и позиционирует себя как частная независимая структура.

Как правило, влиятельные бизнес-структуры или же представители экспертного сообщества обладают уникальными техническими знаниями и компетенциями, пониманием рынка, а также необходимыми информационными ресурсами, что позволяет им либо создавать частные режимы, либо участвовать в многосторонних партнерствах с государственными институтами, направленных на решение конкретных задач в области информационной, но чаще кибер-безопасности. «Лаборатория Касперского» объявила о расширении сотрудничества с Интерполом и Европолом в виде соглашения о кооперации с первым и меморандума о взаимопонимании со вторым. Это объясняется значительным опытом и успехами данной компании в борьбе с компьютерными вирусами и вредоносными программами, вследствие чего правоохранительные агентства все чаще прибегают к частной экспертизе для противодействия киберпреступности.

Другие частные инициативы в области информационной безопасности включают в себя:

- Форум групп реагирования на компьютерные инциденты и безопасность (TheForumofIncidentResponseandSecurityTeams “FIRST”), который координирует работу Групп быстрого реагирования на компьютерные инциденты (CERT), а также занимается разработкой стандартов в области кибербезопасности;
- Инженерный институт электротехники и электроники (TheInstituteofElectricalandElectronicsEngineers “IEEE”), который разрабатывает технические стандарты кибербезопасности во взаимодействии с Национальным институтом стандартизации США;
- ICANN, которая выполняет свои функции по управлению системой доменных имен и адресов Интернета на основании контракта с правительством США
- Международная электротехническая комиссия (International Electrotechnical Commission “IEC”) и Международная организация стандартизации (International Organization for Standardization “ISO”), которые совместно как неправительственные организации создали Совместный технический комитет, разработавший стандарты информационной безопасности для всех типов организаций (ISO/IEC 27001:2005).

Технические решения, принимаемые в рамках вышеуказанных частных организаций, имеют значимые политические последствия в области международной информационной безопасности и управления Интернетом. В отличие от межгосударственного взаимодействия, частные инициативы в сфере информационной безопасности направлены на решение технических не политизированных проблем (таких как выработка стандартов, разработка программ, направленных на борьбу с вредоносным ПО, координация между группами реагирования на компьютерные инциденты - за исключением управления Интернетом, которое в настоящее время политизировано). В условиях секьюритизации и политизации проблематики кибер и информационной

безопасности, переведение проблемы на уровень технической задачи и ее десекьюритизация (в научной литературе также используется термин «технификация»[429]) позволяет передать ее на уровень негосударственных акторов, что облегчает имплементацию выработанных правил.

Следует отметить значительное число международных инициатив по информационной безопасности в последние годы. Описанные выше направления международного сотрудничества на основании методологии исследования могут быть систематизированы следующим образом:

Стадии формирования международных режимов на основании подхода О. Янга	Характер референтного объекта безопасности с позиций теории секьюритизации	Уровни международного сотрудничества
Определение повестки дня	Секьюритизированные	Глобальный уровень: запрет на применение кибероружия, признание права на информационный суверенитет (в сфере контента) Региональный уровень: нет доступной информации[430] Двусторонний уровень: нет доступной информации Транснациональный уровень: нет доступной информации
	Политизированные	Глобальный уровень: международное управление Интернетом; сотрудничество между правоохранительными

[429] Hansen L., Nissenbaum H. Digital disaster, cyber security, and the Copenhagen School //International Studies Quarterly. 2009. №. 4. P. 1155-1175.

[430] В силу секьюритизации проблематики информационной безопасности отдельные международные соглашения могут быть засекреченными. Обозначение «нет доступной информации» означает, что в открытых источниках не удалось найти информацию о взаимодействии в данной области.

		органами государств Региональный уровень: нет доступной информации Двусторонний уровень: нет доступной информации Транснациональный уровень: нет доступной информации
	Неполитизированные	Глобальный уровень: нет доступной информации Региональный уровень: нет доступной информации Двусторонний уровень: нет доступной информации Транснациональный уровень: выработка технических стандартов в сфере управления Интернетом и обеспечения кибербезопасности
Переговоры	Секьюритизированные	Глобальный уровень: применимость международного гуманитарного права к информационной сфере Региональный уровень: отказ от применения кибероружия; признание права на информационный суверенитет Двусторонний уровень:нет доступной информации Транснациональный уровень: нет доступной информации
	Политизированные	Глобальный уровень:

		Помощь в создании цифрового потенциала для развивающихся стран Региональный уровень: нет доступной информации Двусторонний уровень: нет доступной информации Транснациональный уровень: нет доступной информации
	Неполитизированные	Глобальный уровень: нет доступной информации Региональный уровень: отсутствуют Двусторонний уровень: нет доступной информации Транснациональный уровень: нет доступной информации
Имплементация достигнутых соглашений	Секьюритизированные	Глобальный уровень: отсутствуют Региональный уровень: создание мер доверия Двусторонний уровень: создание мер доверия и заключение военно-политических договоренностей Транснациональный уровень: нет доступной информации
	Политизированные	Глобальный уровень: отсутствуют Региональный уровень: сотрудничество между правоохранительными органами государств Двусторонний уровень:

		отсутствуют Транснациональный уровень: управление пространством имен и адресов Интернета
	Неполитизированные	Глобальный уровень: отсутствуют Региональный уровень: выработка технических стандартов в сфере управления Интернетом и обеспечения кибербезопасности Двусторонний уровень: нет доступной информации Транснациональный уровень: выработка стандартов и протоколов безопасности ИТ и транснациональных сетей

Деятельность международных организаций не ограничивается созданием площадок для дискуссий и принятием международно-правовых актов, на двустороннем и региональном уровне зачастую создаются специализированные центры, налажен обмен информацией, принимаются и реализуются программы действий, в том числе совместного реагирования на киберинциденты, проводятся совместные учения – то есть реализуется военно-политическое взаимодействие в сфере информационной безопасности. Таким образом, на региональном и двустороннем уровне международное сотрудничество находится на этапе имплементации достигнутых договоренностей, сформировались региональные режимы информационной безопасности, в рамках таких структур как НАТО, ШОС, АСЕАН. Однако на глобальном уровне в настоящее время международный режим находится на стадии определения переговорной повестки дня, поиска зоны совпадения интересов, что осложняется различиями в национальных интересах

государств и, как следствие, подходах к определению угроз информационной безопасности и механизмов ее обеспечения.Следует отметить, что эффективность региональных режимов не предполагает полного отсутствия информационных и кибер-инцидентов между их участниками (как например, ставшие известными в результате «дела Сноудена» данные о сборе информации спецслужбами США в странах ЕС), но отсутствие серьезных противоречий и конфликтов между их участниками, а также наличие согласованности в поведении, что соответствует определению международного режима, данного С. Краснером как «набора принципов, норм, правил и процедур принятия решений, вокруг которых *сходятся ожидания акторов* в данной области международных отношений»[431].

Следует отметить также интенсификацию двустороннего взаимодействия в условиях отсутствия глобального консенсуса и взаимной уязвимости государств, высоких рисков и высокой цены ошибки. Страны, обладающие значительным киберпотенциалом, заключают договоренности о мерах доверия в кибер- или информационном пространстве.

На уровне транснационального взаимодействия сформировались достаточно устойчивые частные международные режимы, которые регламентируют неполитизированные сферы международного взаимодействия, такие как выработка технических стандартов, а также отдельные политизированные области, такие как управление Интернетом. Вместе с тем, следует отметить, что большая часть некоммерческих структур, выступающих в роли организаторов и исполнителей сложившихся частных режимов, связаны контрактными отношениями с правительством США (напр., ICANN) или же состоят большей частью из граждан США (напр., IETF).

Наращивание информационных потенциалов государствами создает угрозу их использования. Особое значение приобретает выработка мер доверия, необходимых для предотвращения эскалации международных конфликтов в

[431] Krasner S. Structural causes and regime consequence: regimes as intervening variables. // International Regimes. / Ed. by Krasner S. Ithaca, 1983.P. 2.

информационной сфере. В этой ситуации интенсифицируется переговорный процесс, однако, не на глобальном, а на региональном и двустороннем уровне.

«Меры доверия традиционно используются для улучшения отношений между государствами. Они направлены на формирование атмосферы доверия, изменения восприятия угроз, исходящих от взаимодействующих государств, и трансформации межгосударственных отношения и поведения государств с целью предупреждения и урегулирования конфликтов, управления кризисными ситуациями. В информационном пространстве уже были предприняты попытки по формированию мер доверия, однако на двусторонней, а не многосторонней основе»[432]. Наиболее известной попыткой стало создание «горячей линии» между Россией и США в сфере информационной безопасности, недавно схожая договорённость была заключена между Россией и Китаем. В настоящее время обсуждается возможность формирования мер доверия на региональном уровне, в том числе в рамках ОБСЕ, которые могут включать в себя создание центров обмена информацией о информационных угрозах. Меры доверия уже действуют в рамках таких организаций как ОДКБ и НАТО.

Возможно также применение мер повышения прозрачности в целях повышения межгосударственного доверия, относительно того, что другие государства под видом обороны не готовятся к нападению в информационной сфере. Так, на базе ОБСЕ уже проводились серия семинаров по военным доктринам государств-участников, можно расширить подобный опыт на информационную сферу. Подобные меры прозрачности предполагают обмер информации о стратегиях действия в информационном пространстве / киберпространстве, а также информациях о действиях, направленных на обеспечение кибероборонs. Перспективным также видится создание точек обмена информацией и обмен лучшими практиками.

Возможным направлением международного сотрудничества может стать заключение «превентивного» международного договора. Превентивные договоры

[432]Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности // Право и управление. XXIвек. 2014. № 4. С. 47.

запрещают целые классы вооружений, что может послужить моделью для международного сотрудничества в информационной сфере. Страны НАТО выступили с предложением выработать договорный механизм контроля вооружений в информационной сфере, т.е. «конвенцию о кибероружии» с целью обеспечить безопасность киберпространства и не допустить распространения кибероружия[433].

Программный директор Центра стратегических и международных исследований, США предлагает в качестве модели для международных договоренностей по кибер-безопасности использовать «регулятивные договоренности по контролю над вооружениями, аналогичные СНВ 1, которые ограничивают определенный тип вооружений, начиная с НИОКР, затем хранение и применение, а впоследствии демонтаж. Подобные договоренности также ограничивают приобретение или передачу информации о вооружении, в том числе на этапе исследований. Однако, принимая во внимание двойственный характер информационного оружия, маловероятно, что подобные договоренности будут целесообразны»[434], так как практически невозможно доказать, что те или иные разработки в информационной сфере направлены на создание информационных вооружений, а не информационного потенциала для использования в гражданских целях. Более того, спорным является применение таких понятий как «хранение, применение и демонтаж» применительно к кибероружию, так как оно представляет собой программные средства, а не физические системы вооружений.

«Еще один возможный подход к международному сотрудничеству – нормативный. Подобный подход позволяет накладывать ограничения на упреждающее применение информационного оружия. Опыт таких международных соглашений, как Конвенция о запрещении военного или любого иного враждебного использования средств воздействия на природную среду,

---

[433] Arimatsu L. A treaty for governing cyber-weapons: Potential benefits and practical limitations // Cyber Conflict (CYCON). 2012. 4th International Conference on. IEEE, 2012.

[434] Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности // Право и управление. XXIвек. 2014. № 4. С. 48.

которая запрещает упреждающее военное использование целого ряда технологий, может быть использован в отношении информационного оружия. Ряд государств декларировали приверженности принципам отказа от использования военных технологий и в других сферах, однако от подобных заявлений легко отказаться впоследствии, и они не гарантируют, что иные потенциальные агрессоры не готовятся к атакам подобного рода»[435]. Как отмечает Д. Льюис, в информационном пространстве приверженность принципу не использовать кибероружие в целях первого удара, потребует также отказаться от кибершпионажа, так как технологии атаки и кибершпионажа тесно связаны между собой. Это может быть серьезным препятствием к реализации подобных договоренностей, так как большинство государств так или иначе использует кибершпионаж[436].

«Еще одной мерой может быть полное запрещение. Такие конвенции, как Конвенция о запрещении химического оружия или Конвенция о запрещении биологического оружия запрещают владение, хранение и передачу целого класса вооружений. Применение подобного подхода к информационному оружию затруднено в силу того, что отсутствует терминологическое единство в данной области, в частности, не существует консенсусных определений таких понятий, как информационное оружие / кибероружие, а также принимая во внимание тот факт, что многие из технологий информационного воздействия являются технологиями двойного назначения»[437].

Таким образом, специфика информационных видов оружия и кибер-вооружений накладывают определенные ограничения на правовую регламентацию данной области, что в свою очередь, способствует развитию таких механизмов сотрудничества, как меры доверия. В целом, следует отметить, что характер международного взаимодействия по обеспечению информационной безопасности отражает более масштабные процессы, характерные для

[435]Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности // Право и управление. XXIвек. 2014. № 4. С. 48.
[436] Lewis J. Confidence-building and international agreement in cybersecurity // Disarmament Forum. no. 4. 2011. P. 58.
[437] Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности // Право и управление. XXIвек. 2014. № 4. С. 48.

современной международной системы, в частности, тенденцию к регионализации, растущую роль негосударственных акторов, появление новых форматов международного взаимодействия. Более того, геометрия эффективных международных режимов в сфере информационной безопасности отражает структуру современных военно-политических союзов и блоков (с поправкой на уровень развития информационного общества в той или иной стране / регионе и, следовательно, заинтересованность в подобном взаимодействии). При этом специфика информационной сферы обуславливает рост значимости негосударственных акторов, то есть транснационального измерения международного взаимодействие, которое сопрягается с традиционной межгосударственной дипломатией в рамках форматов многоуровневой дипломатии или многосторонних партнерств.

3.2. Специфика международного сотрудничества по обеспечению информационной безопасности: сравнительный анализ

Для выявления специфики международного сотрудничества по обеспечению информационной безопасности целесообразно обратиться к прецедентам международного сотрудничества в других высокотехнологичных областях – контроля над ядерными вооружениями и освоения космического пространства (при учете различий в природе выше обозначенных технологий). Все обозначенные области имеют большое значение для обеспечения национальной и международной безопасности, то есть являются секьюритизированными. Анализ международного сотрудничества в обозначенных областях будет проведен на основании подхода институционального торга при формировании международных режимов, предложенного О. Янгом.

3.2.1. Формирование режима контроля над ядерными вооружениями: сопоставление с сотрудничеством по обеспечению информационной безопасности

Определение повестки дня

Ядерная революция, произошедшая семь десятилетий назад, может позволить сформулировать некоторые выводы относительно перспектив развития международного режима в сфере информационной безопасности.

В частности, сравнение эволюции международного сотрудничества в области контроля над ядерными вооружениями и обеспечения кибербезопасности проводит американский исследователь Д. Най. Анализируя начальный этап развития технологий, Д. Най справедливо указывает, что стратегические исследования в области кибер безопасности в начале 2010-х гг. во многом аналогичны стратегическим исследованиям периода 1950-60-х гг., когда исследователи не могут сделать однозначных выводов о наступательных, оборонительных возможностях новых вооружений, природе сдерживания на международной арене, возможной эскалации конфликтов, нормах поведения, возможности контроля над новым типом вооружений[438].

На начальных этапах формирования международного режима в области контроля над ядерными вооружениями в условиях отсутствия баланса сил США были заинтересованы в закреплении собственного лидерства в новой области, на что были направлены их инициативы по постановке атомной энергетики под международный контроль в соответствии с планом Баруха.

План Баруха, предложенный США на комиссии ООН по атомной энергетике в 1946 году, предполагал введение механизма контроля над ядерными программами присоединяющихся к нему и проведение международных

[438] Nye J. Nuclear lessons for cyber security. Air Univ Press Maxwell Afb Al, 2011.

инспекций. План Баруха, во-первых, предусматривал создание международного Агентства по атомным разработкам (International Atomic Agency) с широкими правами и высокой степенью автономности (решения в агентстве должны были приниматься простым большинством голосов); во-вторых, передачу этому агентству контроля над производством расщепляющихся материалов и передачей их из одних стран в другие; в-третьих, перевод научно-исследовательских разработок в ядерной области под контроль агентства; в-четвертых, предоставление Соединенными Штатами в распоряжение агентства технологической информации по атомной энергии для ее совместного использования странами-участницами. Данный план был воспринят СССР как попытка ограничить развитие ядерного потенциала СССР и сохранить монополию США в ядерной области, в результате чего план не был реализован.

На современном этапе российские официальные лица сравнивают план Баруха в сфере контроля над ядерными вооружениями с созданием ICANN (см. главу 1), причем оба инструмента трактуются как попытка зафиксировать лидерство США в сфере новой перспективной технологии[439].

Однако по мере развития международного режима происходит неизбежное распространение технологии, что в свою очередь, способствует развитию международного режима. После ядерной революции и с развитием средств доставки ЯО в 1960-е гг. сложилась патовая ситуация взаимного гарантированного уничтожения. Важным фактором, способствовавшим формированию международного режима контроля над ядерными вооружениями, стало признание взаимной уязвимости со стороны СССР и США.

Появление водородной бомбы и средств ее доставки у СССР в 1955 г., изменило не только баланс сил, но и представления о возможности победы в потенциальной войне. После Карибского кризиса в 1962 г. в условиях понимания опасностей эскалации конфликта между ядерными сверхдержавами, представления и ожидания государств стали сближаться, что стало основой для

---

[439] Левкович-Маслюк Л. Разреженный воздух киберпространства // Частный корреспондент. 25.05.2009. URL: http://www.chaskor.ru/article/razrezhennyj_vozduh_kiberprostranstva_6736

формирования международного режима в данной области. Важным итогом стало создание мер доверия, прежде всего, «горячей линии» между Москвой и Вашингтоном. Более того, в этот период были заложены основы для режима нераспространения. Пришло понимание, что распространение ядерных технологий не может оставаться мирным и противоречит целям поддержания международной безопасности.

В информационном пространстве сегодня намечается схожая ситуация. Именно осознание уязвимости подталкивает США к признанию военно-политической составляющей угроз МИБ, а также к более активному участию в процессах международного сотрудничества. При этом сходство международного сотрудничества в области контроля над ядерными вооружениями и обеспечения информационной безопасности заключается еще в том, что в обеих областях существует асимметрия между наступательными и оборонительными потенциалами государств – наступление может быть гораздо более эффективным, чем оборона. Уязвимость государств в информационном пространстве также высока, более того, ситуация обостряется сложностью идентификации источника кибератаки. В киберпространстве, DDoS атаки против Эстонии, а также попытка кибersаботажа АЭС в Иране, подсказывают возможные направления кибер-столкновений, однако, по мнению экспертов, не отражают полный спектр их возможностей. Несмотря на то, что некоторые эксперты утверждают, что изменение технических параметров Интернета (протоколов), позволит идентифицировать источники атаки, таким образом, сократив уязвимость наиболее развитых стран, на сегодняшний день тенденции развития сети указывают, что уязвимости в информационной сфере будут лишь возрастать.

Как и в отношении контроля над ядерными вооружениями, в информационном пространстве, процесс международного сотрудничества будет опираться в большей степени на ожидание и восприятие угроз, чем на опыт. Ядерное оружие было применено только против японских городов Хиросима и Нагасаки в 1945 г., вся последующая стратегия сдерживания и инструменты международного сотрудничества выстраивались на основании

опредставленийвозможных характеристиках ядерной войны. В этой связи особенно важно исследовать восприятие угроз и риторику секьюритизирующих акторов для понимания перспектив развития международного режима в сфере информационной безопасности.

Кроме того, подобная ситуация обуславливает высокую роль эпистемических сообществ на этапе формирования повестки дня международного сотрудничества. В рамках режима контроля над ядерными вооружениями подобную роль сыграл Пагуошский комитет, участвовавший в в определении повестки дня и основных форматов международного сотрудничества. Отметим, что схожую роль в рамках режима информационной безопасности играют представители экспертного и инженерного «Интернет-сообщества», однако они в основном представлены исследователями, связанными с США. В этом контексте целесообразно обеспечить большее представительство российских исследователей в экспертных организациях, занимающихся проблематикой управления Интернетом и кибербезопасности.

Переговорный процесс

Как отмечают представители конструктивистской парадигмы, в международной политике значительное влияние оказывают не только материальные факторы, но и интерсубъективные идеи, передающиеся в процессе социализации (обучения). Процесс социализации происходит на основании полученных новых знаний, обучения и опыта и постепенно изменяет восприятие национальных интересов и трансформирует внешнеполитический курс. Так, США и СССР потребовалось несколько десятилетий, чтобы адаптироваться к новым реалиям международной политики, сложившимся в результате научно-технологической революции в ядерной энергетике, пересмотреть свои интересы и осознать взаимную уязвимость и возможность, и целесообразность международного сотрудничества.

Переговоры по созданию международного режима контроля над ядерными вооружениями начались лишь на третьем десятилетии после создания атомной бомбы. Первым формальным документом стал Договор о запрещении ядерных испытаний 1963, он носил в большей степени экологический характер и, кроме того, атомные испытания в атмосфере было легко верифицировать, что упрощало задачу мониторинга имплементации данного соглашения. Следующим значимым соглашением стал Договор о нераспространении ядерного оружия, который ограничил распространение ядерных вооружений к третьим странам. Наиболее развитым механизмом стал договор СНВ-1, который ставил своей задачей контроль количества ядерных вооружений у СССР и США, которые были участниками соглашения и предполагал формирование сложного режима взаимных инспекций, необходимых в условиях взаимного недоверия, что впоследствии стало предметом противоречий. Помимо вышеназванных элементов режим контроля над ядерными вооружениями включает в себя также договоренности и зонах, свободных от ядерного оружия, и меры экспортного контроля, а также ряд других международных договоренностей.

Как и информационные технологии, ядерные технологи породили новые измерения в соотношениях гражданской и военной сферы. Первоначально атомная энергия исследовалась с целью военного использования, однако, вскоре выяснилось, что она может быть использована в мирных целях. Правозащитные и гуманитарные НПО поддерживали мирное использование атомной энергетики, обуславливая это, с одной стороны, энергоэффективностью, а с другой – опасениями развития военной атомной энергетики.

В этих условиях было создано МАГАТЭ, основная цель которого заключалась в контроле над гражданским использованием ядерных технологий. Ограниченные возможности развития атомной энергетики в мирном ключе рассматривались как возможная уступка в переговорном процессе, направленном на ограничение «клуба ядерных государств». Однако, как отмечают исследователи, внешнеполитическая стратегия США в этой области не ограничивалась исключительно национальными интересами. На деятельность

МАГАТЭ оказывали влияние коммерческие структуры, лоббировавшие в том числе, правительство США, которые были заинтересованы в распространении по миру новой технологии, с тем чтобы создать новый рынок. Гражданский сектор играет существенную роль и в развитии информационной сферы, что оказывает влияние на политику государств в данной области и может также формировать нормы, принципы и процедуры принятия решений международного режима.

Определенный интерес также представляет ход переговорного процесса по ДВЗЯИ (Договор о всеобъемлющем запрещении ядерных испытаний). Следует отметить, что изначально переговоры о запрете ядерных испытаний велись, прежде всего, между «великими державами», малые государства могли оказывать давление на позицию ядерных держав в составе коалиций, апеллируя к взятым на себя ранее обязательствам.

Определенная сложность в использовании опыта контроля над ядерными вооружениями заключается в специфике информационного оружия, что затрудняет переговорный процесс в данной области. Так, в информационном пространстве, в отличие от ядерной сферы, сложно отследить источник атаки и точно оценить ее разрушительный потенциал (в отношении ядерных испытаний, как отмечает А. Калядин, «существует возможность надежного обнаружения ядерных взрывов даже сравнительно небольшой мощности»)[440].В этих условиях, для обеспечения международной информационной безопасности требуется более тесное международное взаимодействия для формирования атмосферы доверия, так как в данной области сложнее сохранить союзнические отношения.

По мнению коллектива российских авторов, в современных условиях сложилась ситуация, благоприятствующая формированию международного правового режима нераспространения информационного оружия. «Представляется, что всеобъемлющий режим обеспечения МИБ должен подразумевать установление ограничений, накладываемых на распространение средств информационного воздействия на информационные системы управления

[440]Белоус В.С., Сафранчук И.А. Безопасность и надежность ядерных арсеналов без испытаний. Доклад российского представительства Центра оборонной информации. М.: Воениздат, 2006. С. 9.

критически важными объектами как часть системы международного контроля над вооружениями в целом»[441]. Как отмечают авторы, в этом контексте целесообразно опираться на опыт международных соглашений в области ограничения или запрещения ОМУ, а также Оттавскую конвенцию о запрещении применения, накопления запасов и производства, передачи и применения противопехотных мин от 1998 г. Кроме того, для достижения юридически обязывающих договоренностей впоследствииможнобудет использовать иные формы взаимодействия, такие как международный кодекс поведения (например, по предотвращению распространения баллистических ракет), меморандумы о намерениях (например, в области ракетного нераспространения)[442].

В информационном пространстве наблюдаются схожие процессы в отношении кибервооружений, но не информационной сферы и информационного оружия. Именно этим объясняется ограниченный успех ООН и МСЭ по выработке обязательных норм в области кибер-вооружений на ранних этапах развития режима, и в отношении информационного оружия на современном этапе. Вместе с тем, мы наблюдаем ситуацию, аналогичную формированию мер доверия в атомной сфере между РФ и США, показательно, что «горячая линия» Москва-Вашингтон, созданная после Карибского кризиса, в соответствии с соглашением 2013 года используется для оперативного предупреждения о киберинциндентах.

Схожая риторика секьюритизации на двустороннем уровне – одинаковые речевые практики секьюритизации и общие институты взаимодействия указывают на то, что сотрудничество на двустороннем уровне, вероятно, воспринимается политическими лидерами как схожее и его развитие повторит опыт двустороннего взаимодействия в сфере ядерного нераспространения.

Имплементация достигнутых договоренностей и современные вызовы

[441] Современное состояние и перспективы развития военного сотрудничества Российской Федерации в области международной информационной безопасности / Под общ.ред. С.А. Комова. М.: Министерство обороны, 2014. С 34.
[442] Там же.

Несмотря на схожее влияние на современную стратегическую безопасность, есть важные отличия между ядерными и информационными вооружениями. Одно из различий обусловлено тем, что кибероружие значительно более доступно по сравнению с ядерными вооружениями; отследить передачу соответствующих технологий представляется труднодостижимой задачей. Благодаря мерам контроля удалось добиться определенных успехов в замедлении темпов распространения ядерных технологий и материалов; подобная задача труднореализуема в отношении кибер- и информационных вооружений. Еще одно различие связано с относительным преимуществом нанесения первого удара. В ядерной гонке угроза нанесения одной из сторон выводящего из строя первого удара всегда перекрывалась перспективой потенциального ответного удара; это обстоятельство легло в основу доктрины «взаимного гарантированного уничтожения». В киберпространстве первый удар может быть более быстрым, чем ядерный, при этом идентификация источника атаки затруднена, что осложняет реализацию политику сдерживания.

Краеугольным камнем режима контроля над ядерными вооружениями является Договор о нераспространении ядерного оружия (ДНЯО), вступивший в силу в 1970 г. и продленный бессрочно уже в 1995 г. Несмотря на то, что после 1968 г. ядерное оружие получили три государства Индия, Пакистан, Израиль (а также ЮАР, впоследствии отказавшаяся от ЯО), и, возможно, КНДР, в целом исследователи рассматривают данный режим как эффективный, так как он, несмотря на отдельные нарушения, обеспечивает определенный уровень предсказуемости и стабильности в данной сфере международных отношений[443].

Современный режим контроля над ядерными вооружениями сталкивается с двумя основными группами вызовов (1) «вертикального распространения» – между ведущими ядерными державами в смысле наращивания их ядерных потенциалов и (2) «горизонтального распространения» – в виде расширения числа

[443] Кокошин А.А. Ядерные конфликты в XXI веке (типы, формы, возможные участники). М.: «Медиа-Пресс», 2003; Acton J. M. the Problem with nuclear Mind reading //Survival. – 2009. №. 1. P. 119-142; Goldschmidt P. The Urgent Need to Strengthen the Nuclear Non-Proliferation Regime //Policy Outlook.2006. №. 25.

государств, обладающих ЯО[444]. Кроме того, актуализируются вызовы, связанные с деятельностью негосударственных акторов (опасность попадания ядерного оружия в руки террористических организаций), что обостряется новым витком научно-технического прогресса (как отмечает М.М. Лебедева, создание ядерной бомбы в настоящее время оказывается посильной задачей для группы численностью менее 20 человек при весьма небольших затратах[445]). Как отмечает И.А. Сафранчук, несмотря на проблемы, с которыми сталкивается современный режим ядерного нераспространения, ДНЯО остается его основой[446]. Таким образом, достигнутые в рамках переговорного процесса соглашения основываются на компромиссе между участниками режима и могут считаться весьма эффективными с точки зрения их имплементации.

То же самое можно сказать и о других элементах режима контроля над ядерными вооружениями, в том числе ДВЗЯИ. На сегодняшний день маловероятно, что договор в ближайшее время вступит в силу, вместе с тем, государства-участники не спешат выходить из него, что связано с тем, что данный документ имеет существенный психологический эффект в мировой политике и нарушение его положений воспринимается как внешнеполитическая проблема[447]. Таким образом, режим контроля над ядерными вооружениями включает в себя как формализованные, так и неформализованные нормы, и правила. Вместе с тем, опыт переговорного процесса по ДВЗЯИ, который так и не перешел в фазу формальной имплементации, показывает, что в условиях, когда ставки ключевых участников переговорного процесса высоки (отказ от испытаний фактически означает невозможность совершенствования и развития ядерного потенциала, а также потенциально ставит под вопрос надежность и безопасность существующих ядерных боезарядов) переговорная фаза сотрудничества может

---

[444] Ядерное сдерживание и нераспространение /Под ред. А.Г. Арбатова и В. Г. Дворкина. М.: Московский Центр Карнеги, 2005. С. 12.
[445] Лебедева М.М. Мировая политика. М.: Аспект-Пресс, 2010.
[446] Сафранчук И.А. Режим нераспространения ядерного оружия // Современные глобальные проблемы мировой политики. / Под ред. М.М. Лебедевой. С. 139
[447] Белоус В.С., Сафранчук И.А. Безопасность и надежность ядерных арсеналов без испытаний. Доклад российского представительства Центра оборонной информации. М.: Воениздат, 2006. С. 14.

длиться сколь угодно долго, при этом вырабатываются неформальные правила взаимодействия, которые, однако, не накладывают обязательств на участников режима.

Как уже было показано во второй главе, международное сотрудничество в сфере информационной безопасности на современном этапе сталкивается со схожими проблемами. Опыт многоуровневого сотрудничества в сфере ИКТ может рассматриваться в качестве модели международного сотрудничества, которая впоследствии может применяться в сфере контроля над ядерными вооружениями. При этом, как показывает анализ международного сотрудничества в сфере информационной безопасности, роль государств в подобных форматах должна быть ведущей и координирующей, так как они обладают правосубъектностью в рамках международного права, а также уникальными полномочиями и компетенциями в сфере безопасности («монополия на легитимное насилие» или внутренний суверенитет и независимость на международной арене как атрибуты внешнего суверенитета).

Как показывает доцент МГУ А.В. Фененко, российско-американские отношения в целом подвержены цикличности периодичностью 10-15 лет, связанной с развитием технологий ядерного сдерживания, стремлением добиться лидерства, и, впоследствии, осознанием собственной уязвимости. А.В. Фененко выделяет пять циклов подобного взаимодействия «создание новых правил взаимодействия в стратегической сфере, модернизация стратегических потенциалов в рамках новых правил, появление представлений о возможности достижения стратегического превосходства, наступление серьезного военно-политического кризиса и возобновление переговоров о ревизии правил взаимодействия в стратегической сфере»[448]. Если применять данную модель к сотрудничеству в сфере международной информационной безопасности, то можно сделать следующий вывод: международное сотрудничество по обеспечению информационной безопасности находится на этапе признания

[448] Фененко А.В. Военно-техническая модернизация и «циклы» сближения между США и Россией // Международные процессы. 2011. № 2. URL: http://www.intertrends.ru/twenty-sixth/005.htm

взаимной уязвимости и выработки новых правил взаимодействия в киберпространстве, которое всеми участниками рассматривается как стратегически важная область.

3.2.2. Сравнение международного сотрудничества в сфере информационной безопасности с международно-правовым режимом космического пространства

Определение повестки дня

История освоения околоземного космического пространства человеком насчитывает более 50 лет. Исследование регулирования космического пространства представляют особый интерес, так как в современных условиях космос и информационная сфера в значительной мере пересекаются – так, значительная часть услуг связи (как военного, так и гражданского характера) предоставляется с опорой на космические системы.

Космическое пространство, как и информационное пространство, стало ареной межгосударственного соперничества и противоборства. Хорошо известна фраза Д. Кеннеди «Кто имеет превосходство в космосе, будет иметь превосходство и на Земле». Вместе с тем, освоение космоса на протяжении всей истории было тесно связано с национальной и международной безопасностью, а также описанной выше ядерной безопасностью, так как именно стремление двух противостоящих государств в атомной сфере донести до территории противника атомную бомбу обусловило первые попытки попасть в околоземное космическое пространство[449]. Таким образом, данная область международного взаимодействия также является секьюритизированной.

На протяжении Холодной войны ключевыми акторами в космосе являлись государства. Изначально, в виду технической сложности данной сферы, лишь два государства обладали потенциалом освоения космического пространства – СССР

[449] Бирюков А.В. Современные международные научно-технологические отношения. М.: РОСНОУ, 2014. С. 279

и США. (на сегодняшний день не менее 12 государств развивают собственные космические программы)[450].

Первоначально СССР и США конкурировали между собой за лидерство в освоение космоса, причем на первых этапах СССР одерживал победы (запуск искусственного спутника Земли в 1957 г., отправка человека в космос в 1961 г.). Однако впоследствии борьба шла с переменным успехом. В 1975 г. стыковка кораблей «Аполлон» и «Союз» символизировала сотрудничество сверхдержав в освоении космоса, хотя и не прекратила полностью соперничество между ними.

На начальных этапах формирования режима также значительную роль сыграли представители экспертного сообщества. Как отмечает А.А. Кокошин «первая половина 1970-х гг. стала временем появления огромного количества аналитических записок и докладов о будущем космических исследований. Выводы советских и американских ученых оказались неутешительными»[451]. Достижение стратегического превосходства в космосе на тот период оказалось нереализуемой задачей.

Однако государства изначально рассматривали космос как арену стратегического противоборства, что обуславливает секьюритизацию данной области. Вместе с тем, и в данной области значимую роль в развитии международного взаимодействия сыграл Карибский кризис 1962 года. Как отмечает российский исследователь В. Мизин, еще при открытии первого этапа переговоров по разоружению советское руководство увязывало вопросы ограничения стратегических вооружений и разоружения на «космическом треке»[452]. В свете Карибского кризиса стороны осознавали, что размещение ядерного оружия в космосе чревато непредсказуемыми военно-стратегическими последствиями и вероятностью ужасающих технических катастроф[453].

---

[450] Космос: оружие, дипломатия, безопасность / Под ред. А. Арбатова, В. Дворкина ; Моск. Центр Карнеги. — М. : Российская политическая энциклопедия (РОССПЭН), 2009. — 175 с.URL: http://carnegieendowment.org/files/12659outer_space_arbatov.pdf

[451] Россия и международная безопасность в космосе / Под ред. А.А. Кокошина. М.: URSS, 2013. С. 9.

[452] Мизин В. Опыт переговоров по немилитаризации космоса. // Космос: оружие, дипломатия, безопасность / Под ред. А. Арбатова, В. Дворкина ; Моск. Центр Карнеги. М.: Российская политическая энциклопедия (РОССПЭН), 2009. С. 88.URL: http://carnegieendowment.org/files/12659outer_space_arbatov.pdf

[453] Там же.

Таким образом, в сфере освоения околоземного космического пространства, в отличие от ядерной безопасности, на начальных этапах развития технологии сложился паритет возможностей между двумя сверхдержавами, что ускорило темпы формирования международного режима в данной области – то есть процесс согласования повестки дня занял меньшее количество времени. Спецификой космической сферы также является техническая сложность и экономическая емкость освоения космоса, в связи с чем, уязвимость государств в данной области изначально была ниже, чем в сфере ядерной безопасности. В этих условиях значимость проблемы была ниже, чем в сфере ядерной энергетике, а восприятие равенства возможностей подталкивало государства к международному взаимодействию в данной области. В этой ситуации этап определения переговорной повестки дня был пройден достаточно быстро в рамках созданного в 1958 г. Управления ООН по вопросам космического пространства. К 1963 году относятся первые международные договоренности по космосу.

В октябре 1963 г. была принята резолюция ГА ООН о запрете вывода на орбиту любых объектов, с ядерным оружием, первоначально зафиксированная как договоренность между США и СССР. Позднее, в декабре 1963 г. ГА ООН была принята Декларация правовых принципов, регулирующих деятельность государств по исследованию и использованию космического пространства, которая, несмотря на то, что она не имеет обязательного характера заложила основы для дальнейших договоренностей в данной области – в частности, было зафиксировано, что космическое пространство не подлежит присвоению национальными государствами[454]. Также в 1963 году был принят Договор о запрещении испытаний ядерного оружия в атмосфере, космическом пространстве и под водой.

[454] Декларация правовых принципов, регулирующих деятельность государств по исследованию и использованию космического пространства. Резолюция ГА ООН 1962 (XVIII). Нью Йорк, 13.12.1963. URL: http://www.un.org/ru/documents/decl_conv/declarations/outerspace_principles.shtml

Переговорный процесс

Межгосударственные отношения в космическом пространстве характеризуется значительной взаимозависимостью. Применительно к космическому пространству, в силу его специфики, традиционные нормы об ограничении вооружений были бы малоэффективными, в том числе по причине сложности верификации и имплементации (в отличие от ядерной сферы).

Международное сотрудничество столкнулось с проблемой размывания границ между гражданскими и военными сферами –космические технологии, как и информационные в большинстве своем являются технологиями двойного назначения. Это, в свою очередь создавало препятствия для международного сотрудничества, так как затрудняло определения таких понятий как оружие, противоборство, кроме того, это затрудняет возможность ограничить или запретить использование тех или иных технологий и проследить за имплементацией соглашений об ограничении вооружений.

В этой ситуации государства пошли по пути выработки гибких договоренностей и вынесения спорных вопросов за скобки. Подобный подход мог бы быть применим и к информационной сфере. Значительная часть договоренностей по космосу была направлена на повышение прозрачности и доверия между государствами.

Первым документом, регламентировавшим исключительно использование космического пространства, стал Договор по космосу (Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела) 1967 года. Договор устанавливает запрет на национальное присвоение космического пространства, включая Луну и другие небесные тела, вывод на орбиту, размещение в космосе и установку на небесных телах объектов с ЯО и иными видами оружия массового поражения. Таким образом, космическое пространство признается общим

достоянием всего человечества. Как отмечают А. Арбатов и В. Дворкин, принятие договора основывалось на всеобщем интересе государств, так как угроза потери управления над оружием, инцидентов и катастроф с непредсказуемыми последствиями была очевидна и весьма велика. Основываясь на безусловном общем интересе всех стран, Договор не содержал детальных определений предмета соглашения, методики запрета и мер контроля[455]. Договор 1967 г. носит общий характер и в нем достаточно пробелов и лакун в регулировании, что признается многими экспертами[456]. Отдельные пробелы впоследствии были восполнены в таких международных договоренностях, как Соглашение о спасении космонавтов, возвращении космонавтов и возвращении объектов, запущенных в космическое пространство (1968), Конвенция о международной ответственности за ущерб, причиненный космическими объектами (1972), Конвенция о регистрации объектов, запускаемых в космическое пространство (1976), Соглашение о деятельности государств на Луне и других небесных телах (1984)[457]. Правда, последнее ратифицировано лишь несколькими государствами, среди которых нет ни одного с существенной космической программой. Кроме того, был принят ряд резолюций ГА ООН по космосу, которые послужили правовой базой для принятия вышеуказанных документов.

Российские исследователи проводят параллели между международно-правовым регулированием на ранних этапах освоения космического пространства и развития информационного общества[458]. В обоих случаях развитие новых технологий формирует взаимозависимость и порождает вызовы и угрозы гражданского и военного характера. Разработка правовой базы, регулирующей поведение государств в космическом пространстве в целях обеспечения международной безопасности, шла поэтапно, параллельно разрабатывались общие принципы поведения и проблемы ограничения отдельных действий

---

[455] Арбатов А., Дворкин В. Заключение. // Космос: оружие, дипломатия, безопасность / Под ред. А. Арбатова, В. Дворкина ; Моск. Центр Карнеги. М.: Российская политическая энциклопедия (РОССПЭН), 2009. С. 88.URL: http://carnegieendowment.org/files/12659outer_space_arbatov.pdf

[456] Там же.

[457] Инновационные направления современных международных отношений / Под ред. А.В. Крутских, А.В. Бирюкова. М.: Аспект-Пресс, 2010. С. 183.

[458] Федоров А.В. Информационная безопасность в мировом политическом процессе. М.: МГИМО, 2006.

государств в данной сфере (напр., запрещение ядерных испытаний, а впоследствии и размещения ЯО в космосе). Для регулирования чувствительных, спорных направлений деятельности, которые сложно было вписать в рамки строго обязательных международно-правовых документов, были найдены приемлемые формы деклараций и принципов (как, например, Принципы, касающиеся использования ядерных источников энергии в космическом пространстве и др.). Как представляется, опыт международного сотрудничества по космосу и использования таких инструментов, как принципы поведения и кодексы, вынесения спорных вопросов за скобки, может быть продуктивно использован в отношении глобальной информационной сферы.Вместе с тем, ключевое отличие киберпространства заключается в том, что значимость проблематики значительно выше, так как информационное оружие значительно более доступно по сравнению с космическими технологиями, с большей вероятностью может быть использовано без катастрофических последствий для международной безопасности. Это в свою очередь затрудняет переход от стадии определения повестки дня к переговорной стадии по обеспечению информационной безопасности на международном уровне.

Имплементация достигнутых соглашений и современные вызовы

Международно-правовой режим космического пространства основан на нормах «мягкого права», которое представляет собой гибкий инструмент международного сотрудничества в условиях различных государственных интересов. Несмотря на то, что нормы, связанные с недопустимостью размещения ОМУ в космосе не оспариваются и выполняются государствами, существующие договоренности не предусматривают системы контроля, что связано со спецификой космической деятельности. Кроме того, в международных договоренностях есть лакуны, допускающие, в частности, размещение обычных вооружений в космосе. На современном этапе международный режим космического сотрудничества, так же как и режим ядерного нераспространения

сталкивается с рядом сложностей – прежде всего, связанных с растущей ролью негосударственных акторов. Кроме того, значительная часть международных договоренностей разрабатывалась в годы Холодной войны и устарела в связи с развитием научно-технического прогресса.

Современные вызовы, с которыми сталкивается международный режим по использованию околоземного пространства, могут быть систематизированы следующим образом:

1. Милитаризация, которая также подкрепляется растущим числом государств, способных создавать собственные космические программы.
2. Приватизация – растет число частных инициатив в космической сфере, следовательно, усиливается влияние негосударственных акторов, которые не участвуют в международном режиме.
3. Размытые границы между наступательным и оборонительным потенциалом в космической сфере – что зачастую ведет к тому, что наступательный потенциал государства представляют как оборонительные меры.
4. Ассиметричный характер угроз – нападение дешевле и эффективнее защиты, как в технологическом, так и в материально-экономическом измерениях.[459].

Можно сказать, что вызовы, с которыми сталкивается международный режим по использованию околоземного космического пространства во многом аналогичным вызовам, которые стоят на пути международного сотрудничества по обеспечению информационной безопасности (милитаризация, асимметрия возможностей, растущая роль негосударственных акторов, сложности в разграничении оборонительного и наступательного потенциала).

В отличие от режима нераспространения ядерного оружия, который большинство авторов предлагает сохранить с некоторыми модификациями, международно-правовой режим космического пространства зачастую трактуется

[459]Securing Outer Space: International Relations Theory and the Politics of Space / Ed by Bormann N., Sheehan M. Routledge, 2009 P. 2

как устаревший, несоответствующий современному этапу научно-технического прогресса и развития мировой политики. Таким образом, эффективность данного режима ставится под вопрос[460]

В настоящее время начался новый этап переговорного процесса по адаптации международного режима в космической сфере к новым реалиям технологического и международно-политического взаимодействия. Это связано, прежде всего, с практической возможностью и целесообразностью использования космических систем в современных международных отношениях с целью достижения стратегического превосходства. В этих условиях, новый международный режим находится на стадии согласования повестки дня. Как отмечают А. Арбатов и В. Дворкин, переговоры по вопросу демилитаризации космоса в настоящее время находятся на этапе определения предмета возможных соглашений[461].

В то время как Россия и Китай с 2008 г. продвигают договора о предотвращении размещения оружия в космическом пространстве, применения силы или угрозы силой в отношении космических объектов (ДПРОК), который предусматривает запрет на размещение в космосе оружия любого вида и на какие-либо силовые действия в отношении космических объектов, США выступают против подобной инициативы (и ряда иных, связанных с ней инициатив). Подобная позиция США обусловлена стремление обеспечить лидерство в военном использовании космического пространства, закрепив стратегическое превосходство[462].

В настоящее время в условиях милитаризации космоса обостряется межгосударственная конкуренция.По мнению доцента МГУ А.В. Фененко, включение информационного пространства в категорию "общих пространств", по аналогии с космическим, отнюдь не означает сотрудничество государств по

---

[460] См. напр.: Tannenwald N. Law versus power on the high frontier: The case for a rule-based regime for outer space //Yale Journal on International Law. 2004. URL: http://drum.lib.umd.edu/bitstream/1903/7902/1/tannenwald.pdf

[461] Арбатов А., Дворкин В. Заключение. // Космос: оружие, дипломатия, безопасность / Под ред. А. Арбатова, В. Дворкина ; Моск. Центр Карнеги. — М. : Российская политическая энциклопедия (РОССПЭН), 2009. С. 88.URL: http://carnegieendowment.org/files/12659outer_space_arbatov.pdf

[462] Инновационные направления современных международных отношений / Под ред. А.В. Крутских, А.В. Бирюкова. М.: Аспект-Пресс, 2010. С. 187.

обеспечению безопасности и развития глобальной информационной сферы.Если в начале 90-х гг. прошлого века была распространена точка зрения, согласно которой освоение "новых пространств", таких как околоземный космос, объединяет государства и способствует размыванию их суверенитета, то современные тенденции демонстрируют обратное… взаимодействие в рамках "общих пространств" предполагает сегодня не столько межгосударственное сотрудничество в их освоении, сколько соперничество за принципы их раздела»[463].

Рассмотренные выше примеры международного сотрудничества в высокотехнологичных областях предлагают аналогии для анализа международного сотрудничества по обеспечению информационной безопасности. Все рассмотренные области (ядерное нераспространение, освоение космического пространства, информационная безопасность) являются секьюритизированными. При этом в роли секьюритизирующих актороввыступают государства, великие державы. Государства во всех случаях являлись ведущими акторами, однако не единственными, на их действия оказывали влияние бизнес-структуры, НКО, представители экспертного сообщества (в рамках концепции секьюритизации подобные субъекты взаимодействия рассматриваются как функциональные акторы). Представители экспертного сообщества играли значимую роль на начальных этапах формирования международных режимов. Важным условием развития международного сотрудничества стало признание общей уязвимости между участниками режимов.Таким образом, в исследованных высокотехнологических областях наблюдается явление, которое можно обозначить как «технологический изоморфизм» в мировой политике - сходство моделей международно-политического взаимодействия и сотрудничества по поводу регулирования области мировой политики, возникающей в связи с развитием новых технологий, проявляющееся на различных этапах зрелости

[463] Фененко А.В. Международное соперничество за освоение общих пространств // Международные процессы. 2010. № 1. URL: http://www.intertrends.ru/twenty-second/003.htm

данных технологий. Так, на начальных этапах развития технологий, как правило, сильна роль экспертного сообщества (также называемого эпистимеческим сообществом), на последующих этапах усиливают свое влияние государства и бизнес-структуры. Необходимым условием развития международного взаимодействия является признание общей уязвимости, а международные кризисы, как правило, способствуют переходу взаимодействия на этап имплементации достигнутых соглашений. Кроме того, следует отметить, что характерный для истории и философии технологий подход технологического детерминизма не вполне адекватен для описания отношений между новыми технологиями и мировой политикой. Скорее наблюдается взаимное влияние технологий и мировой политики, при этом технологии всегда вписаны в более широкий социальный и политический контекст, а природа их регулирования отражает характер международной системы, политической модели мира, которая носит Вестфальский характер и в этой связи носит консервативный характер, что и объясняет феномен изоморфизма.

При этом «технологический изоморфизм» не абсолютен, следует отметить также и различия. Во-первых, различия затрагивают природу технологий, различные направления их использования. Во-вторых, если режим ядерного нераспространения и международно-правовой режим освоения космоса формировались в период стабильной биполярной системы Холодной войны и поэтому являются глобальными по своей сути, то в отношении информационной безопасности в условиях отсутствия консенсуса между великими державами и не сформировавшейся системы «равновесия страха» в информационной сфере мы наблюдаем скорее формирование нескольких региональных режимов, что отражает, с одной стороны, специфику информационныхтехнологий как объекта регулирования на международном уровне, ас другой – тенденцию к регионализации мировой политики и, как следствие, информационного пространства, рассмотренную в 1 главе настоящего исследования.

Можно предположить, что в краткосрочной перспективе глобальный режим информационной безопасности будет развиваться по аналогии с международно-

правовым режимом космического пространства, что обусловлено схожестью условий (неэффективностью оборонительных стратегий, общей уязвимостью, стремлением государств сохранить «свободу рук» в отношении военного использования новых перспективных технологий) и будет использовать в основном инструменты «мягкого права». Однако, двусторонние договоренности о мерах доверия (между США и Россией, США и Китаем и др.) и растущая технологическая сложность информационного оружия и, как следствие, его труднодоступность для большинства государств, в долгосрочной перспективе могут привести к формированию более «жесткого» международного режима, во многом схожего с режимом нераспространения ядерного оружия, ориентированного на закрепление привилегированного положения великих держав.

3.3. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности

3.3.1. Позиции участников переговорного процесса и перспективы достижения глобального консенсуса по обеспечению информационной безопасности

Международное сотрудничество по обеспечению информационной безопасности на глобальном уровне наталкивается на противоречия в государственных интересах. Именно от позиций влиятельных государств зависит перспектива формирования глобального режима по обеспечениюинформационной безопасности. Как отмечают исследователи международного сотрудничества, зачастую отсутствие институционально или формально закрепленного режима отражает интересы отдельных государств, стремящихся сохранить лидерство в какой-либо области. Схожей стратегией может быть поддержка формирования множества разрозненных организаций и институтов, регламентирующих взаимодействие в отдельной области международных отношений, так как это позволяет выбирать различные нормы и

правила взаимодействия, зафиксированные в этих соглашениях, в зависимости от ситуативных интересов[464]. Как представляется подобная ситуация сложилась в сфере обеспечения международной информационной безопасности и управления Интернетом, где сформировалось множество функциональных и ряд региональных режимов (см. пп. 3.1 настоящего исследования).

Российские и зарубежные эксперты в качестве ключевых субъектов международного сотрудничества в области информационной безопасности называют следующие страны – США, Россия, Китай, а также страны ЕС (Великобритания, Франция и Германия)[465], отмечая, что они обладают наибольшим потенциалом в данной области. Более того, они также выступают в качестве наиболее активных участников переговорного процесса по МИБ. Ниже проанализированы их позиции по вопросу информационной безопасности.

В российской научной литературе по вопросам информационной безопасности зачастую акцентируется внимание на противоречиях, которые существуют между США и Россией в данной области, которые рассматриваются как ключевое препятствие на пути к международному сотрудничеству. Причинами противоречий являются, с одной стороны, классическая межгосударственная конкуренция и борьба за влияние на международной арене, а с другой – различие в потенциалах и, как следствие, интересах в информационной сфере (ценности также играют определенную роль, однако, как показывает т.н. «дело Сноудена» приверженность общим ценностям не отменяет межгосударственной конкуренции и борьбы за власть – США были готовы использовать превосходство в информационном потенциале, чтобы упрочить влияние над союзниками). США являются лидером в сфере ИКТ и не заинтересованы в ограничении «свободы рук». Официально на международном уровне в отношении управления интернетом США выступают за сохранение многоуровневой модели управления интернетом, сложившейся в рамках PTI и

[464]Т.н. стратегия “forum shopping” (см. Busch M. L. Overlapping institutions, forum shopping, and dispute settlement in international trade //International Organization. 2007. №. 04. С. 735-761)

[465] Giles K., Hagestad W. Divided by a common language: cyber definitions in Chinese, Russian and English //Cyber Conflict (CyCon), 2013 5th International Conference on. – IEEE, 2013. – С. 1-17.

ICANN, формирование свободного от государственного контроля глобального информационного пространства, резко критикую практику выделения суверенных сегментов глобальной сети и укрепления «цифрового суверенитета». В сфере информационной безопасности США, с одной стороны, развивают наступательный и оборонительный информационный потенциал (при этом разрабатывая теоретические концепции достижения информационного превосходства и его соотнесения с глобальным лидерством), а с другой – выступают против адаптации международного права к информационной сфере. Так, США и их союзники по НАТО поддерживают идею разработки правил применения существующего корпуса международного права к информационной сфере, таким образом, легитимируя информационные войны, но помещая их в правоые рамки. В ходе переговоров США вплоть до недавнего времени делали основной акцент исключительно на технологических аспектах защиты информационных сетей, борьбы с терроризмом и преступностью и выступали за исключение из международных документов указаний на военно-политическую составляющую проблемы (в последние годы США признают наличие военно-политических угроз, однако отказываются обсуждать проблему регулирования информации, передаваемой по информационным сетям).

А.В. Бедрицкий систематизировал ключевые интересы, лежащие в основе позиции США по проблеме информационной безопасности следующим образом:

«1. Военное использование киберпространства целесообразно и будет иметь большое значение. Соединённые Штаты не намерены связывать себя какими-либо ограничениями на развёртывание, испытания и использование военных возможностей в этой сфере в целом. В дальнейшем в интересах защиты критически важных инфраструктур характеристики конкретных кибернетических угроз будут детализироваться и по ним могут быть подписаны международные соглашения. Однако вопрос о том, насколько такие соглашения будут ограничивать наступательный потенциал США и, соответственно, будет ли целесообразным международное обсуждение этих вопросов, должен решаться в ходе всесторонних исследований и моделирования.

2. Соединённые Штаты будут настаивать на том, чтобы эти соглашения не исключали возможности осуществлять возмездие (сдерживание) в случае проведения против них кибернетических атак другими странами. Они также будут последовательно выступать за право предупреждать кибернетические атаки, поскольку считают такие действия активной защитой своих инфраструктур.

3. Поскольку в случае проведения кибератаки достаточно трудно выявить страну-агрессора, Соединённые Штаты, возможно, будут заинтересованы в подписании многостороннего соглашения, определяющего пропорциональность ответа на кибератаку, исходя из её масштаба, продолжительности и потенциальной угрозы для гражданских объектов. Это, естественно, потребует выработки в той или иной мере режима верификации»[466].

Показательно, что в киберстратегии Министерства обороны США от 2015 г. в качестве основных угроз безопасности США указаны агрессивные действия России и Китая в киберпространстве, отмечены также угрозы, исходящие от Ирана и КНДР, а также негосударственных акторов – кибертеррористов (прежде всего, ИГИЛ (ДАИШ)) и киберпреступников. Еще в 2011 г. киберпространство было объявлено полем боя, то в 2015 году был определен порог ущерба кибератак, в ответ на которые будут предприняты ответные меры, в том числе с использованием обычных вооружений[467].

Изменение позиций США по вопросу обеспечения информационной безопасности стало следствием изменения баланса сил вследствие стремительного развития киберпотенциала Китая. В исследовательском сообществе США ведутся дискуссии о формах возможных киберстолкновений с Китаем[468], в аналитических отчетах отмечается значительное число кибератак со стороны китайских хакеров на критические инфраструктуры США[469].

---

[466] Бедрицкий А.В. Международные договорённости по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. 2012. №4. URL: http://www.riss.ru/images/pdf/journal/2012/4/10 .pdf

[467]The Department of Defense Cyber Strategy. Washington, April, 2015. URL: http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[468]Cyber war and competition in the China-US relationship //Remarks delivered at the China Institutes of Contemporary International Relations. – 2010. – T. 13. URL:

Россия же стремится ограничить возможные риски, связанные с информационным пространством таким образом, укрепив национальную и международную безопасность. Кроме того, Россия добивается закрепления принципа невмешательства в информационное пространство – согласно проекту Конвенции об обеспечении международной информационной безопасности, представленной на рассмотрение ООН Россией «Каждое государство вправе устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством»[470]. И хотя в документе указывается, что государства должны защищать свободу слова в Интернете и «не вправе ограничивать доступ граждан к информационномупространству», делается важная оговорка: правительства могут вводить ограничения «в целях защиты национальной и общественной безопасности»[471].

По сравнению с российскими исследователям, зарубежные эксперты вплоть до 2016 года с большей озабоченностью отмечали обострение противоречий между США и Китаем в сфере обеспечения информационной безопасности[472].Вместе с тем в 2016 году в рамках общего охлаждения отношений между США и Россией проблематика кибербезопасности стала отдельным пунктом двусторонней повестки дня. США обвиняли Россию в государственной поддержке хакеров, которые взломали электронные ресурсы Агентства национальной безопасности США, базу денных Всемирного антидопингового агентства (WADA), а также получили доступ к личной переписке кандидата на

---

http://dspace.africaportal.org/jspui/bitstream/123456789/28852/1/Cyber%20war%20and%20competition%20in%20the%20China-US%20relationship.pdf?1

[469]Half of Critical Infrastructure Providers Have Experienced Perceived Politically Motivated Cyber Attacks. Press Release: Symantec. 2010. URL: http://finance.yahoo.com/news/Half-ofCritical-iw-478930509.html?x=0&.v=1

[470] Конвенция об обеспечении международной информационной безопасности (концепция). // МИД России. Официальный сайт. 22.09.2011. URL: http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument

[471]Тамже.

[472]Lieberthal K., Singer P. Cybersecurity and U.S. - China Relations. // Jonh L. Torton China Institute in Brookings, 2012. URL:http://www.brookings.edu/~/media/Research/Files/Papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.PDF; Half of Critical Infrastructure Providers Have Experienced Perceived Politically Motivated Cyber Attacks. Press Release: Symantec. 2010. URL: http://finance.yahoo.com/news/Half-ofCritical-iw-478930509.html?x=0&.v=1; Lewis J. A. Cyber war and competition in the China-US relationship // Remarks delivered at the China Institutes of Contemporary International Relations. – 2010. – T. 13. URL: http://dspace.africaportal.org/jspui/bitstream/123456789/28852/1/Cyber%20war%20and%20competition%20in%20the%20China-US%20relationship.pdf?1

пост президента США Х. Клинтон. В этой ситуации проблема обеспечения кибербезопасности стала предметом активных переговоров между странами. Однако по большинству вопросов позиции государств расходятся.

Россия и США продвигают два различных видения проблемы обеспечения информационной безопасности. Если Россия, как и Китай, выступает за государственное регулирование информационной сферы и обеспечение информационной безопасности на основании международных договоров, то США предпочитают частную модель регулирования и уклоняются от вопросов регулирования контента. Отметим, что Китай также является одним из важных игроков в данной области. Несмотря на то, что в официальных документах Китая не сформулированы однозначные определения угроз кибербезопасности[473], анализ внешнеполитической позиции, подписанных договоренностей и выступлений официальных лиц позволяют сделать вывод, что Китай придает особое значение опасности распространения ценностей через Интернет и выступает за сохранение «цифрового суверенитета». Также как США и Россия, Китай рассматривает информационную безопасность как составляющую национальной безопасности, при этом в опубликованной Министерством обороны КПК «Белой книге по безопасности» 2012 г. признается право Китая отвечать на кибер-атаки вплоть до использования обычных вооружений[474]. Вместе с тем, Китайские официальные лица напрямую не обвиняют США в совершении кибер-атак на критические информационные инфраструктуры, хотя, неофициально многие аналитики отмечают, что большая часть атак осуществляется при помощи компьютеров, чьи IP-адреса зарегистрированы на территории США[475].

Схожесть позиций России и Китая подтверждается тем фактом, что 8 мая 2015 года Россия и Китай подписали соглашение между правительствами двух стран о сотрудничестве в области обеспечения международной информационной безопасности. В документе зафиксировано общее понимание угроз в

[473] Swaine M. D. Chinese Views on Cybersecurity in Foreign Relations //China Leadership Monitor. 2013. T. 42. C. 1-27.
[474]Цит по: Swaine M. D. Chinese Views on Cybersecurity in Foreign Relations //China Leadership Monitor. 2013. T. 42. C. 1-27.
[475] Там же.

информационной безопасности - использование ИКТ в террористических целях, для вмешательства во внутренние дела государств, подрыва суверенитета, политической и экономической стабильности, разжигания межнациональной и межконфессиональной вражды, совершения правонарушений и преступлений[476]. Столь же тесные отношения в сфере кибербезопасности связывают Россию лишь с партнерами по ОДКБ. По мнению западных экспертов, данное соглашение можно трактовать как стремление государств подорвать лидирующие позиции США в сфере управления Интернетом и Интернет-индустрии[477].Отметим, что Россия и Китай реализуют совместные инициативы в сфере информационной безопасности в рамках ряда международных организаций, в том числе ООН, БРИКС, ШОС. Однако, по мнению экспертов, Китай занимает выжидательную позицию в отношении политики США в информационной сфере[478], несмотря на то, что противоречия между США и Китаем носят не только политический, но и экономический характер – именно США обвиняют в изоляции китайских ИТ-компании, в частности Huawei, от глобальных рынков[479].

Развивающиеся страны в большинстве своем солидаризируются с позицией России, поддерживая идею необходимости государственного контроля над национальными сегментами интернета, инернационализации регулирования интернета и формировагия глобального всеобъемлющего режима международной информационной безопасности. «Для развивающихся стран в ходе международных переговоров, как правило, приоритетными являются вопросы информационного развития и сокращения «цифрового разрыва», помощи в создании «цифровых потенциалов», несмотря на то, что в последние годы вопросы информационной безопасности стали подниматься в контексте

---

[476] Сообщение для СМИ. О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности // МИД России. Официальный сайт. 8.05.2015. URL: http://www.mid.ru/brp_4.nsf/newsline/2C7A7D0752AAB2B843257E3F003F2204

[477] См. напр.: Risen T. China, Russia Seek New Internet World Order // US News and World Report. 14.05.2015. URL: http://www.usnews.com/news/articles/2015/05/14/china-russia-seek-new-internet-world-order

[478] См. напр.: Ибрагимова Г. Стратегия КНР в области управления Интернетом и информационной безопасности // Индекс безопасности. 2013. № 1. URL: http://www.pircenter.org/articles/1106-strategiya-knr-v-oblasti-upravleniya-internetom-i-obespecheniya-informacionnoj-bezopasnosti

[479] Huawei. The company that spooked the world // The Economist. 4.08.2012. URL: http://www.economist.com/node/21559929

«цифрового разрыва», эта проблематика является относительно самостоятельной и мало связанной с основной повесткой дня в области международной информационной безопасности»[480].

Что же касается союзников США по НАТО, следует отметить, что «поход стран ЕС, которые также выступают в роли влиятельных игроков в глобальном информационном пространстве, трактуется исследователями как схожий с подходом США, в силу, прежде всего, союзнических обязательств по НАТО, а также значительной взаимозависимости в экономических аспектах развития Интернет-индустрии. Традиционно, страны ЕС выказывали озабоченность, прежде всего, относительно защиты от информационных угроз для экономики»[481]. Вместе с тем, следует отметить, что среди союзников по НАТО, есть разногласия в сфере информационной безопасности и управления интернетом. Как показали международные переговоры в ходе NetMundial, а также Группы правительственных экспертов ООН по международной информационной безопасности 2014 – 2015 гг. европейские страны, прежде всего, Германия и Франция тяготеют к более независимой политике в отношении информационной безопасности, в частности, в сфере управления Интернетом они поддерживают интернационализацию контроля над этой технологией. Эксперты связывают подобное изменение позиций ряда европейских стран с разоблачениями Э. Сноудена, указавшего на факт использования США своих преимуществ в информационной сфере в целях получения политических и экономических и политических целей в ущерб интересам стран ЕС[482].

Таким образом, стороны выдвигают заведомо неприемлемые друг для друга требования, завышая первоначальные позиции на переговорах, с тем, чтобы добиться более выгодного итогового соглашения. «Как показывает опыт развития международных режимов в других высокотехнологичных областях, один актор не может навязывать другим нормы, принципы и правила поведения в долгосрочной

---

[480]Зиновьева Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности // Вестник МГИМО – Университета. 2016. № 4. С. 238.
[481]Там же. С. 237.
[482] Сноуден: АНБ следит за учреждениями и гражданами Евросоюза // Интерфакс. 08.03.2014. URL: http://www.interfax.ru/world/363552

перспективе. Динамичный характер развития Интернета и подвижность социо-экономической среды указывают на то, что США, хотя и выступали в роли гегемона на начальном этапе развития режима постепенно утрачивают подобные позиции, т.к. их роль в рамках режима все чаще ставится под вопрос другими государствами. Изначальные позиции гегемона ставятся под вопрос вмешательством национальных и международных акторов, ростом их потенциала, ассиметричными угрозами и, кроме того, динамической природой Интернета»[483].

В настоящее время открываются новые возможности формирования глобального режима международной информационной безопасности. Долгое время США сознательно ограничивали возможности формирования глобального правового режима информационной безопасности. Однако изменение характера угроз информационной безопасности привело к тому, что наиболее развитая в информационном плане держава оказалась крайне уязвимой. Как показывает российский исследователь, сотрудник СПбГУ Р.В.Болгов, американская военная мощь, созданная для укрепления национальной безопасности, и информационно-технологичные вооружения как составляющие этой мощи на деле способствовали провоцированию конфликтности (в т.ч. за счет попыток противников США создать ядерное оружие) и только ослабили безопасность, для обеспечения которой они предназначались[484].

«Несмотря на то, что ряд противоречий отошел на второй план (США согласились с некоторыми из российских предложений, признав наличие военно-политических угроз в области информационной безопасности, а также необходимость правового регулирования данной области) наметились новые проблемы: так, западные страны выступают не за полную демилитаризацию информационного пространства, что соответствует российским интересам, но за международно-правовое регулирование киберконфликтов, с целью ограничить возможность использования информационного оружия в отношении особенно

---

[483] Зиновьева Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности // Вестник МГИМО – Университета. 2016. № 4. С. 237.

[484] Болгов Р.В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях // Дисс. … ученой степени кандидата политических наук. СПб: СПбГУ, 2011.

уязвимых критических инфраструктур, имеющих ключевое значение для безопасности населения, таких, например, как информационные системы, обеспечивающие работу госпиталей, и пр.»[485]. Позицию стран НАТО, прежде всего США, по вопросу международно-правового регулирования военно-политического аспекта информационной безопасности отражает опубликованное 19 марта 2013 года Таллиннское руководство. Данный документ, подготовленный группой экспертов Центра совместной кибероборонь НАТО в Таллинне, посвящен вопросам применения международного права к конфликтам в информационной сфере, прежде всего, в ее технологическом измерении[486].

Согласно официальной позиции России, данное руководство допускает возможность милитаризации информационного пространства, в то время как Россия подчеркивает необходимость полного запрета информационного оружия. Таким образом, данный документ можно рассматривать как «пробный шар» на пути легитимации кибервойн, которые рассматриваются как допустимое средство разрешения межгосударственных противоречий, но закрепляется их место в правовом поле.

Вместе с тем, как утверждает О. Демидов, российский и западный подходы не обязательно противоречат друг другу. Россия выступает за подчинение поведения государств в информационном пространстве специальному своду универсальных и юридически обязывающих норм. Разница между двумя подходами заключается в том, что они рассматриваются через призму разных установок и задач. Если Россия и ее союзники видят свою миссию в том, чтобы не допустить межгосударственных киберконфликтов и вывести такие явления за рамки приемлемых действий на международной арене, то Таллиннское руководство – документ, не несущий такой задачи.

Сближение и гармонизация двух подходов – задача на отдаленную перспективу что обусловлено, прежде всего, дефицитом доверия между

[485]Зиновьева Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности // Вестник МГИМО – Университета. 2016. № 4. С. 237.
[486] Tallinn Manual on the International Law Applicable to Cyber Warfare / ed. by M. Schmitt – N.Y.: Cambridge University Press, 2013.

ключевыми участниками переговоров. Заключение двусторонних соглашений по информационной безопасности может сформировать необходимую для продолжения переговоров атмосферу доверия.

«Определенным препятствием для многостороннего переговорного процесса в данной области является то, что для многих государств проблематика военно-политического использования ИКТ является чувствительной, и они не всегда готовы открыто обсуждать ее.Весьма спорным также является вопрос включения вопросов регулирования контента информационных сетей в сферу обсуждения в ходе международных переговоров. Россия настаивает на использовании терминов «информационная безопасность», «информационное пространство», предполагающих более широкий подход к определению референтного объекта безопасности, – в этом случае объектом безопасности являются не только сетевое оборудование и программное обеспечении, но и более широкие, социально-гуманитарные аспекты развития информационного общества. США же настаивают на использовании термина «кибербезопасность», что предполагает обеспечение исключительно безопасности компьютерных сетей. Однако и в данной области есть определенное развитие: дискуссии в ходе деятельности последний ГПЭ ООН и обсуждения проектов вышеназванных резолюций позволили выработать некий вариант нейтральной терминологии. В тексте резолюций рассматриваемая проблематика формулируется вне рамок западной лексики кибербезопасности и, по большей части, не в терминах «обеспечения МИБ». Поиски участниками ГПЭ взаимоприемлемых формулировок с целью нахождения компромисса привели к тому, что тексты резолюций обращены к проблематике «ИКТ в контексте международной безопасности», «злонамеренного использования ИКТ» и др. Таким образом, вынося спорные терминологические вопросы за скобки, удается выработать хрупкий компромисс»[487].

[487]Зиновьева Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности // Вестник МГИМО – Университета. 2016. № 4. С. 237.

В рамках складывающегося режима обеспечения международной информационной безопасности общие интересы государств и бизнеса заключаются в том, чтобы установить хрупкую атмосферу доверия и укрепить он-лайн отношения, и это достигается при помощи принципов, норм, правил и процедур принятия решений для защиты конфиденциальности, целостности и доступности, достоверности, приватности информации. И принятие правил поведения государств в данной сфере может быть важным шагом на пути к развитию международного сотрудничества. Отметим, что еще в 2011 г. Россия предложила свод правил поведения в сфере ИКТ на рассмотрение ООН как проект Конвенции об обеспечении международной информационной безопасности. В документе делается особый акцент на суверенитете в информационной сфере и невмешательстве во внутренние дела[488]. Схожий свод правил вносился на рассмотрение ООН и по линии ШОС в 2011 и в 2015 гг. Однако, США и ЕС долгое время не были готовы обсуждать подобные правила поведения, рассматривая их как попытку ограничить свободу в Интернете и ввести цензуру в сети. В настоящее время страны Запада поддерживают инициативу введения правил, однако полагают, что правила не должны быть обязывающими и не должны привести к разделению Интернета на национальные сегменты. Отметим, что страны ЕС в последние годы все более открыто высказываются в поддержку идеи правил поведения, однако, не поддерживая идею «цифрового суверенитета». Более того, данная инициатива нашла поддержку у Индии, которая, как отмечает сотрудник ПИР-центра О.В. Демидов, «опасается киберугроз со стороны Китая»[489].

Однако, несмотря на то, что сегодня все ключевые участники переговорного процесса согласны с необходимостью выработки правил поведения, позиции относительно содержания правил, сферы их действия, а также обязательств из них

---

[488] Конвенция об обеспечении международной информационной безопасности (концепция). // МИД России. Официальный сайт. 22.09.2011. URL: http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument

[489] Демидов О.В. Обеспечение международной информационной безопасности и российские национальные интересы // Индекс Безопасности. 2013. № 1. С. 136. URL: http://www.pircenter.org/media/content/files/10/13559089230.pdf

проистекающих существенно различаются. «Таким образом, международные переговоры по формированию глобального режима управления Интернетом находятся на стадии определения повестки дня, и важно, что Россия выступает в роли инициатора обсуждения многих проблем, так как это дает важные преимущества в переговорном процессе. В настоящее время, несмотря на сложность и новизну рассматриваемой проблематики, не только развивающиеся, но и развитые страны поддерживают инициативу международно-правового регулирования глобальной информационной сферы»[490].

Несмотря на активизацию переговоров по вопросам информационной безопасности, маловероятно, что консенсусное решение будет найдено в ближайшей перспективе. Можно согласится с А.В. Бедрицким, по мнению которого «гораздо более вероятно, что Соединённые Штаты будут пытаться всячески продвигать свою модель кибернетической безопасности»[491]. Если проводить аналогии с режимами в других высокотехнологичных областях, ситуация может измениться вследствие международного кризиса, который коренным образом изменит представления государств о собственной уязвимости, подтолкнув к пониманию необходимости международного сотрудничества.

3.3.2. Перспективы развития международного режима в сфере управления Интернетом

Проблема управления Интернетом в ходе переговорного процесса все чаще увязывается с вопросами международной информационной безопасности. От того, на каких принципах будет организовано управление сетью Интернет, которая выступает в качестве системообразующей инфраструктуры глобального информационного общества, будут зависеть политические и экономические

[490]Зиновьева Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности // Вестник МГИМО – Университета. 2016. № 4. С. 238.
[491] Бедрицкий А.В. Международные договорённости по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. 2012. №4. URL: http://www.riss.ru/images/pdf/journal/2012/4/10 .pdf

характеристики глобального информационного пространства, что не может не влиять на международную информационную безопасность.

Как было показано в 1 главе настоящего исследования, в настоящее время сложился государственно-частный режим управления Интернетом, в рамках которого функции технической координации пространства имен и адресов Интернета возложены на некоммерческую организацию PTI, дочернюю организацию ICANN, зарегистрированную в США и формально подчиняющуюся законам США. В настоящее время все большее количество государств оспаривают роль ICANN и PTI в управлении Интернетом, видя в ней инструмент влияния США.

Отметим, что режим управления Интернетом исторически формировался при существенном влиянии экспертного сообщества (т.н. «Интернет-сообщества») исследователей и инженеров, однако в настоящее время государства стремятся играть в управлении Интернетом более существенную роль. Поскольку США и их союзники не были уверены в том, каким образом следует осуществлять управление Интернетом в тот период, когда он только приобретал популярность, они предоставили свободу действий экспертам. Как заявляет Э. Хаас: «В условиях неопределенности, когда вся власть сосредоточена в руках одного государства, и когда эпистемические сообщества успешно консолидировали влияние в доминирующем государстве, тогда действия этого государства могут быть модифицированы в соответствии с убеждениями представителей эпистемического сообщества. Режим все равно будет формироваться под контролем гегемона, однако его содержание будет отражать взгляды эпистемического сообщества»[492]. Подобные режимы, как правило, называют режимами «смешанного происхождения».

М. Франда в своей книге «Управление Интернетом: формирование международного режима» анализирует процесс развития международного режима на основании предложенных О. Янгом стадий, которые каждый режим проходят в

[492] Haas P. Epistemic Communities and International-Policy Coordination - Introduction. //International Organization. 1992. No. 46 (1). Pp. 1-35.

ходе формирования: определение повестки дня; международные переговоры; операционализация достигнутых соглашений. Наибольшее внимание М. Франда уделяет первой стадии, процессам определения международной повестки дня в области управления Интернетом. Он анализирует ту роль, которую эпистемические сообщества и даже отдельные лица играли на ранних этапах формирования режима, и приходит к выводу, что именно частные лица и некоммерческие организации, обладающие на тот период монополией на определенные виды информации, во многом определяли международную повестку дня в области управления Интернетом. При этом эпистемические сообщества, не смотря на свободу действий, никогда не обладали полной автономией, их ключевые решения направлялись правительством США, на гранты которого они осуществляли свою деятельность.

Однако по мере того, как количество пользователей новой технологии возрастала, на правительство США, возрастала экономическая, политическая, культурная, социальная и др. значимость сети, и, следовательно, государства во все большей степени осознавали потенциал технологии и стремились принимать участие в управлении Интернетом. Желая избежать передачи управления Интернетом к одной из существовавших на тот период межправительственных организаций, США решили передать функции управления Интернетом к частной некоммерческой организации, сохранив при этом контрольные полномочия по отношению к ее деятельности. Следовательно, этими же соображениями правительство США руководствовалось и 2016 году при создании PTI–она позволила сохранить критические ресурсы технической координации интернета внутри США и избежать передачи функций IANA к межправительственной организации. При этом эпистемические сообщества инженеров и разработчиков интернета сохраняют свое влияние и в рамках институционального дизайна PTI, как это было показано в 1 главе.

Сложившийся в рамках ICANN и PTI государственно-частный режим управления Интернетом не только не соответствует интересам большинства государственных акторов (в том числе и РФ), которые видят в нем

институционализацию доминирования США в информационном пространстве. ICANN на протяжении всей своей истории с момента создания подвергалась существенной критике, причем главным объектом являются ее «особые отношения» с Департаментом торговли США, который сохраняет за собой контрольные функции по отношению к данной организации. Создание PTI не смогло придать легитимности сложившейся системе управления интернетом, в том числе, в глазах официальных лиц Российской Федерации, ответственных за стабильное и бесперебойное функционирование российского сегмента интернета[493].

Таким образом, PTI не удалось стать легитимной институциональной структурой управления Интернетом на межгосударственном уровне. Однако остальным организациям «Интернет-сообщества» пока удается сохранять свои позиции в процессах управления. Стремление правительств принимать участие в процессах управления Интернетом сохраняет свою актуальность.

Остановимся более подробно на прогнозах развития режима управления Интернетом в целом и ICANN в частности, предлагаемых различными исследователями и аналитиками. Большая часть исследователей соглашается с тем, что Дубайская конференция МСЭ 2012 г. ознаменовала начало нового этапа в данном процессе, который будет характеризоваться утерей США своего влияния и усилением позиций правительств других государств.

Очевидно, что США не могут игнорировать обеспокоенность мирового сообщества в отношении их односторонней политики в сфере регулирования Интернета. Со стороны Вашингтона была сделана уступка – предоставление ICANN независимости от Департамента торговли, что позволило избежать наиболее нежелательно варианта – интернационализации управления Интернетом и перехода функций ICANN к МСЭ. Однако, предоставив ICANN формальную независимость, США, тем не менее, сохранили контроль над инфраструктурой Интернета благодаря рыночному влиянию (большая часть крупных компаний,

---

[493] Щеголев И. Весь наш интернет уязвим к внешнему воздействию. // РБК. 27.03.2017. URL: http://www.rbc.ru/newspaper/2017/03/27/58d3bc559a79471ca8c1fbbd

работающих в Интернет-пространстве, имеет американскую принадлежность), экономическому потенциалу (американские корпорации управляют доменными именами общего уровня, на которых зарегистрирована значительная часть доменов), а также управлению корневыми серверами, большая часть из которых так и останется на территории США.

Складываются благоприятные условия, чтобы передать контроль управления Интернетом к МСЭ. Высока вероятность того, что в ходе саммита по вопросам развития информационного общества под эгидой ООН, запланированного на 2020 г., США уступят лидирующие позиции в сфере управления Интернетом. Этому способствует не только растущая уязвимость в сфере информационной безопасности, но и сложившиеся международная ситуация в данной области.

Проблематика управления Интернетом тесно связана с вопросами обеспечения международной информационной и кибер-безопасности. От того, на каких принципах будет организован глобальный Интернет, будет зависеть облик глобального информационного пространства, в том числе, в контексте его безопасного функционирования. Управление Интернетом и обеспечение международной информационной безопасности увязывает Россия, так как, согласно официальной позиции, монопольное положение США создает дополнительные угрозы международной информационной безопасности; схожей позиции придерживается Китай.

3.3.3. Направления адаптации международного права к информационной сфере

С точки зрения основателя неправительственной организации «DiploFoundation», которая специализируется на ИКТ измерении дипломатической службы, Й. Курбалиа, существуют как минимум два подхода к адаптированию существующих норм международного права к информационному пространству.

Первое направление можно обозначить как «реальное» право». Оно основано на предположении, что Интернет не обладает качественной спецификой по сравнению предшесвовашими ему инструментоами коммуникации. Он бесспорно быстрее своиз предшественников, но, однако, это не означает, что он обладает новым качеством, которое требует новым правил и норм регулирования. Поэтому все существующие релевантные нормы и правила могут быться использованы по сути в неизменном виде для регулирования Интернетом.

Второе направление, напротив, исходит из предположения, что Интернет все же представляет из себя качественно новое являение, для которого необходимо разрабатывать новые нормы и правила, так называемое «кибреправо». Основным аргументом в обоснование такого подхода яввляет ссылка на невероятную скорость передачи данных по Интернету. Она создает новое качество коммуникации, которую необходимо управлять по-новому[494].

С теоретической точки зрения, сделать выбор между этими двумя позициями довольно сложно, т.к. определенная правда есть в каждой из них. Однако на практике, как указывыает Й. Курбалиа, доминирует «реальное право». При этом очевидно, что по некоторым узкотехническим вопросам необходима разработка абсолютно новых норм[495].

«Вместе с тем, в современных условиях проблема адаптации международного права к информационной сфере является крайне политизированной, что связано с межгосударственными противоречиями, обозначенными в предыдущем параграфе.Несмотря на специфические характеристики ИКТ, вытекающие из Устава ООН общепризнанные принципы международного права jus cogens и соответствующие нормы международного права, а именно невмешательство во внутренние дела государств и неприменение силы и угрозы силой остаются незыблемыми как в традиционном, физическом, так и в новом, цифровом пространстве.

[494]Курбалиа Й. Управление Интернетом. М.: Координационный центр национального домена сети Интернет, 2010. С. 85.
[495]Там же.

Остановимся более подробно на вопросах применения существующего корпуса международного гуманитарного права к информационной сфере, прежде всего, к применению информационного оружия против объектов критической информационной инфраструктуры. Информационные войны по многим параметрам отличаются от противостояния государств в «реальном» мире. Тем не менее, это не отменяет необходимости нормативно-правовой регламентации. Многие из положений международного гуманитарного права были выработаны применительно к обычным условиям ведения войны и в современных условиях требуют доработки.

Право вооруженных конфликтов, несмотря на свою оторванность от политической практики, определяет правила цивилизованного ведения вооруженных действий. Международное гуманитарное право обладает лишь ограниченной применимостью по отношению к информационным конфликтам. Между тем существует насущная потребность в выработке правил регулирования конфликтов в информационной сфере. Это связано с тем, что информационные атаки по своим последствиям становятся все более масштабными, создавая реальную угрозу безопасности государству. Более того, участниками информационных конфликтов могут быть не только государства, но и неправительственные участники, в том числе террористические группировки»[496].

На сегодняшний день сложился целый корпус документов международного права, регламентирующих международные отношения в ходе вооруженного конфликта, получивший название международного гуманитарного права. Данная отрасль права обладает существенным потенциалом регулирования отношений в условиях информационного противоборства, несмотря на то что термин «защита критических инфраструктур» не используется в документах, лежащих в основе международного гуманитарного права. Положения, касающиеся защиты гражданских обхектов в ходе вооруженных конфликтов вполне применимы к информационной сфере: «гражданские объекты не должны являться объектом

[496]Зиновьева Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности. // Вестник МГИМО – Университета. 2016. № 4. С. 243.

нападения или репрессалий»[497]. Конвенции предписывают исключение такого рода объектов из возможных объектов атаки, а также постоянную защиту и бережное обращение. В том случае, если статус гражданских объектов утрачивает свою силу, атакующая сторона обязуется сделать должное предупреждение.

«Таким образом, международное гуманитарное право лишь в ограниченной мере применимо к защите объектов критической информационной инфраструктуры, используемой в гражданских целях, как, например, информационные ресурсы и системы, обеспечивающие работу госпиталей и больниц. Могут применяться положения Дополнительного протокола Гаагской конвенции 1907 г., запрещающие подвергать нападению или уничтожению объекты, необходимые для выживания гражданского населения (запасы пресной воды, запасы продуктов питания и др.). Однако, среди критических информационных инфраструктур можно выделить лишь незначительное количество систем, используемых исключительно в гражданских целях, что сужает применимость норм гуманитарного права. Большая часть может использоваться как в гражданской, так и в военной сферах, вследствие чего нормы права нуждаются в доработке»[498].

В большинстве случаев в информационной сфере сложнее определить гражданские объекты, так как в наступательных и оборонительных операциях могут быть задействованы гражданские объекты. Согласно источникам международного гуманитарного права, военным относятся объекты, «которые в силу своего характера, размещения, назначения или использования вносят эффективный вклад в военные действия и полное или частичное разрушение, захват или нейтрализация которых при существующих в данный момент обстоятельствах дает явное военное преимущество»[499].

---

[497]Дополнительный протокол I к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооруженных конфликтов (Протокол I). Женева, 8 июня 1977 г. (ст. 52)

[498]Зиновьева Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности. // Вестник МГИМО – Университета. 2016. № 4. С. 244.

[499]Второй протокол к Гаагской конвенции о защите культурных ценностей в случае вооруженного конфликта 1954 года. Гаага, 26 марта 1999 г. (ст. 1).

«Почти все государства рассматривают информационную безопасность объектов критической инфраструктуры как проблему национальной безопасности. Отметим, что, несмотря на пробелы в международном праве, информационная безопасность в большинстве стран регулируется внутренними законодательными нормами. Пионерами в данном контексте являются США, в которых после событий 11 сентября 2001 г. безопасность критических информационных инфраструктур начинает рассматриваться в контексте антитеррористической стратегии. Вполне эффективно могут применяться положения Дополнительного протокола №1 Гаагской конвенции 1907 г., запрещающие подвергать нападению или уничтожению объекты необходимые для выживания гражданского населения (запасы пресной воды, запасы продуктов питания и др.).

В настоящее время многие элементы национальной инфраструктуры находятся в сфере владения частного сектора и не являются собственностью государства. Поэтому важным в организации системы ее эффективной защиты является сотрудничество правительственных ведомств, общественных организаций, с привлечением коммерческих структур, осуществляющих деятельность в ключевых секторах национальной критической инфраструктуры. Очевидно, что опыт внутригосударственного регулирования должен быть использован при выработке международно-правовых норм»[500].

«Изучение вопроса применимости и достаточности международного гуманитарного права для правового регулирования действий с применением информационного оружия осуществимо только при понимании того, что признается существование и возможность использования информационных систем как оружия, а организованное противоборство с его использованием признается как война. В настоящее время международное сообщество приходит к такому пониманию. Страны склонны признавать свою уязвимость в информационной сфере, и проявляют готовность принимать международно-

[500]Зиновьева Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности. // Вестник МГИМО – Университета. 2016. № 4. С. 244.

правовые документы, регулирующие и ограничивающие возможность агрессивных действий в информационной сфере»[501].

В этих условиях необходима адаптация норм права, чтобы компьютеры и программные коды можно было классифицировать как системы вооружения. Термин «информационное оружие» используется в ряде международных документов, принятых в рамках ШОС и СНГ[502]. Например, согласно ст. 1 Соглашения между Правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16.07.2009 главной угрозой международной информационной безопасности является «разработка и применение информационного оружия, подготовка и ведение информационной войны», ее признаками являются «... воздействие на системы транспортировки, коммуникаций и управления воздушными, противоракетными и другими видами объектов обороны, в результате чего государство утрачивает способность обороняться пред лицом агрессора и не может воспользоваться законным правом самозащиты, нарушение функционирования объектов информационной инфраструктуры, в результате чего парализуются системы управления и принятия решений в государствах, деструктивное воздействие на критически важные структуры»[503]. «Подобный подход может быть использован международным сообществом в качестве основы для выработки общепризнанного определения информационного оружия»[504].

Подводя итог рассмотрению применимости международного гуманитарного права к информационным войнам, отметим, что, несмотря на то что большая часть его положений разрабатывалась в отношении обычных вооружений, его положения разрабатывались с целью гуманизировать войну, избежать страданий мирного населения, поэтому если они и устарели, то лишь формально, но не по сути. Как отмечает российский эксперт А.В. Федоров, «в информационном

---

[501]Там же.

[502] См. напр.: Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2009 г.

[503]Там же.

[504]Зиновьева Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности. // Вестник МГИМО – Университета. 2016. № 4. С. 245.

обществе доминируют интересы государств, прежде всего, интересы политические, и их столкновение ведет к противоборству, в наиболее острой форме – информационной войне. Тем не менее, это не отменяет регламентации международных отношений нормами международного публичного права»[505].

3.4. Информационная безопасность России в современных международных отношениях

Значимость национальных интересов России в области информационной безопасности особо подчеркивает тот факт, что они упоминаются в целом ряде официальных документов последних лет, среди которых Стратегия национальной безопасности до 2020 года[506], Стратегия развития информационного общества[507], Концепция внешней политики Российской Федерации[508], Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года[509] и др. В 2012 г. в МИД России была создана специальная должность – специального координатора по политическим вопросам использования ИКТ, которую занял профессор МГИМО МИД России А.В. Крутских. В 2014 году на него были возложены обязанности специального представителя Президента России по вопросам международного сотрудничества в области информационной безопасности.

В настоящее время осуществляются утвержденная Президентом в 2007 году «Стратегия развития информационного общества в Российской Федерации». Государственная программа «Информационное общество 2011–2020» ставит своей целью развитие информационных технологий в России, а также ее

[505]Федоров А.В. Информационная безопасность в мировом политическом процессе: учеб пособие. М.: МГИМО(У), 2006. - С. 138.

[506]Стратегия национальной безопасности Российской Федерации до 2020 года: указ Президента РФ № 537 от12.05. 2009. URL:http://www.mid.ru/ns-osndoc.nsf/0e9272befa34209743256c630042d1aa/8abb3c17eb3d2626c32575b500320ae4?OpenDocument

[507]Стратегия развития информационного общества в Российской Федерации. Утверждена 07.02.2008. Пр-212. URL:http://www.mid.ru/ns-osndoc.nsf/0e9272befa34209743256c630042d1aa/453f799b9fe0637cc32573f3002b2558?OpenDocument

[508]Концепция внешней политики Российской Федерации. Утверждена 30.11.2016. URL: http://www.scrf.gov.ru/documents/2/25.html

[509] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Утв. Президентом Российской Федерации Пр. № 1753 от 01.08.2013. / Совет Безопасности РФ. URL:http://www.scrf.gov.ru/documents/6/114.html

вхождение в глобальное информационное общество[510]. Программа охватывает следующие направления: создание электронного правительства, преодоление цифрового неравенства, развитие новых технологий связи.

На сегодняшний день Россия является одним из наиболее динамичных и устойчиво растущих ИКТ-рынков в мире[511]. Начиная с 2002 г. количество активных пользователей Интернета в РФ неуклонно возрастает. Активно развивается и российский сегмент Интернета. Домен «.RU» по числу сайтов стал 10-м среди всех доменов верхнего уровня в мире. Домен «.RU» также является одним из самых быстрорастущих мировых доменов, а домен «.РФ» остается крупнейшим интернационализованным доменом в мире[512]. Вклад Интернет-сектора в национальную экономику составил порядка двух процентов от ВВП[513]. Однако в российском секторе Интернета есть свои проблемы: по уровню проникновения Интернета мы отстаем от развитых стран. Так, в Канаде, США и Австралии 70% населения регулярно пользуются Интернетом[514].

В «Стратегии национальной безопасности РФ до 2020 г.» информационная безопасность рассматривается в качестве одной из важнейших составляющих национальной безопасности страны[515]. Интернет видится как канал распространения экстремизма и терроризма, навязывания чуждой идеологии и внешнеполитической пропаганды.

Национальные интересы России в информационной сфере впервые были сформулированы в 2000 г. в «Доктрине информационной безопасности России». Согласно данному документу, национальные интересы в информационной сфере включают в себя интересы общества, личности и государства; на основе

---

[510] О государственной программе Российской Федерации "Информационное общество (2011-2020 годы): распоряжение Правительства Российской Федерации от 20 октября 2010 г. № 1815-р // Российская газета. 16.11.2010. URL:http://www.rg.ru/2010/11/16/infobschestvo-site-dok.html

[511] Электронная Россия (2002-2010 годы): Федеральная целевая программа // Юридическая компания «Интернет и право»: 2010. URL:http://www.internet-law.ru/intlaw/laws/e-rus.htm

[512]Российское доменное пространство 2012: итоги и перспективы развития // Координационный центр национального домена сети Интернет. 2012. URL:http://www.cctld.ru/files/stats/report_ru-2013_rus.pdf

[513]Россия онлайн: влияние Интернета на российскую экономику: отчет BostonConsultingGroup. 1.05.2011. URL:http://img.rg.ru/pril/article/48/57/59/000111333.pdf

[514]Internet World Stats.Usage and population statistics. URL:www.internetworldstats.org

[515]Стратегия национальной безопасности Российской Федерации до 2020 года: указ Президента № 537 от 12.05.2009.
URL:http://www.mid.ru/ns-osndoc.nsf/0e9272befa34209743256c630042d1aa/8abb3c17eb3d2626c32575b500320ae4?OpenDocument

национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства.

«Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества»[516].

Можно выделить следующие составляющие национальных интересов РФ в Интернет-пространстве: национальная безопасность, экономические и социально-политические интересы. Вследствие трансграничной природы Интернета интересы России в данной области имеют не только национальную, но и международную составляющую.

Актуальное понимание Россией угроз в области информационной безопасности можно проследить на основании принятой в декабре 2014 года

[516]Доктрина информационной безопасности Российской Федерации. Утверждена 09.09.2000. Пр-1895. URL:http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm

Военной доктрины Российской Федерации, где указано, что «наметилась тенденция смещения военных опасностей и военных угроз в информационное пространство и внутреннюю сферу Российской Федерации»[517]. По сути, это стало реакцией России на массовые протесты в 2014 г. в Украине, когда социальные сети и блоги активно использовались для координации протестного движения.

Однако, несмотря на внимание к проблеме информационной безопасности, «закрытия» Интернет-пространства не произошло. В 2014 г. был принят ряд инициатив в области информационной политики, направленных на то, чтобы обеспечить устойчивость российского сегмента Интернета, в том числе от внешних воздействий. В частности, был принят законопроект, который предписывает всем операторам персональных данных (включая Интернет-компании) обрабатывать и хранить их строго на территории страны. Кроме того, принят закон о регистрации блоггеров, обсуждается возможность создания дублирующей инфраструктуры Интернета в России. Данные решения повлекли за собой ожидаемую негативную реакцию со стороны Интернет-компаний: так, штат разработчиков Google был выведен из России. В мае 2015 г. в Вооруженных силах РФ были сформированы специальные войска информационных операций, которые должны защитить российских военных от кибертерроризма и шпионажа[518]. В 2016 году была принята новая редакция Доктрины информационной безопасности России. В документе особое внимание уделено соотношению военно-политического и экономического измерения информационной безопасности. В частности, отмечается необходимость поддрежки российских компаний, работающих в области ИКТ и электронной промышленности, создание условий для их конкурентоспособности на глобальных рынках[519].

---

[517] Военная доктрина Российской Федерации. Утв. Президентом РФ 25.12.2014. Пр-2976. URL: http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/2a959a74cd7ed01f432569fb004872a3!OpenDocument

[518] В России появились войска информационных операций, сообщил источник в Минобороны // Newsru.com. 12.05.2014. URL: http://www.newsru.com/arch/russia/12may2014/information.html

[519] Доктрина информационной безопасности Российской Федерации. Утверждена указом Президента № 646 от 5.12.2016. URL: http://www.scrf.gov.ru/documents/6/5.html

Таким образом, экономическое измерение проблематики также играет значимую роль. В отчете по информационной безопасности, составленном Hewlett-Packard (HP) и Ponemon Institute, утверждается, что в среднем ущерб от кибератак в России составляет 3,3 млн долларов на одну организацию или компанию. Это вдвое меньше, чем в Великобритании и в четыре раза меньше, чем в США. Чаще всего жертвами кибератак становятся промышленные компании, энергетические и финансовые структуры[520]. Развитие информационно-коммуникационных технологий (ИКТ) рассматривается в качестве инструмента повышения конкурентоспособности экономики, повышения эффективности государственного управления и местного самоуправления. Более того, в условиях санкций, введенных рядом стран Запада, импортозамещение в сфере ИКТ видится как возможный двигатель экономического развития, также рассматривается возможность выхода российских ИТ-компаний на азиатские рынки.

Таким образом, сохраняется и развивается видение, сформулированное в Основах государственной политики в области международной информационной безопасности на период до 2020 года, где Россия обозначила опасность вмешательства во внутренние дела суверенного государства посредством ИКТ, нарушение общественной стабильности, разжигание межэтнической, межнациональной розни. В числе основных внешних опасностей для России в военной доктрине выделены «использование информационных и коммуникационных технологий в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности». К числу внутренних опасностей отнесена «деятельность, направленная на насильственное изменение конституционного строя Российской Федерации, дестабилизацию внутриполитической и социальной ситуации в стране, дезорганизацию

[520] 2014 Global Report on the Cost of Cyber Crime // Hewlett Packard. URL: https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf

функционирования органов государственной власти, важных государственных, военных объектов и информационной инфраструктуры Российской Федерации»[521]. Кроме того, к числу угроз информационной безопасности отнесена зависимость от внешних источников технологического развития в сфере информационных технологий. Этот подход начал аткивно реализовываться на общегосударственном уровне в 2014-2015 гг., когда началась реализация политики импортозамещения в сфере ИКТ и в иных высокотехнологичных областях[522].

Официальные документы и выступления государственных деятелей свидетельствуют, что Россия заинтересована в демилитаризацию информационной сферы, стремясь к поддержанию сложившегося военно-стратегического статус-кво в мире. Такой важный документ как «Основы государственной политики в области международной информационной безопасности на период до 2020 года» провозглашает основной целью политики России в области международной информационной безопасности подержку формирования международного правового режима, который бы позволил создать необходимые условия для формирования системы международной информационной безопасности. Вероятность реализации данной задачи несомненно повысится, если будут созданы условия, снижающие риск использования ИКТ для осуществления актов агрессии против государственного суверенитета, территориальной целостности и подрыва международного мира и безопасности в целом. Концепция внешней политики Российской Федерации утверждает, что Россия будет прикладывать все усилия, чтобы на базе ООН были выработаны правила международного взаимодействия в области международной информационной безопасности[523].

---

[521] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Утв. Президентом Российской Федерации Пр. № 1753 от 01.08.2013. / Совет Безопасности РФ. URL:http://www.scrf.gov.ru/documents/6/114.html

[522] Самофалова О. США и ЕС испугались российского импортозамещения // Взгляд. 17.04.2015. URL: http://www.vz.ru/economy/2015/4/17/740632.html

[523] Концепция внешней политики Российской Федерации. Утверждена 30.11.2016. URL: http://www.scrf.gov.ru/documents/2/25.html

Российская дипломатия не ограничивается испольованием глобальных форумов для продвижения свой повестки в сфере международной информационной безопасности, но и активно задействует возможности межправительственных организаций. В частности, вопросы управления Интернетом дипломаты обсуждают в таких организациях, как ООН, МСЭ, ЮНЕСКО, ШОС, СНГ, Совет Европы. Нередко наши дипломаты инициируют обсуждение на данных международных площадках вопросы информационной безопасности, вопросов правового регулирования использование ИКТ и управления Интернетом. Россия придерживается принципов приемственности и поэтапности в посторонии международно-правового режима информационной безопасности. Строительство должно вестись по направлению снизу вверх. Сначала должны быть достигнуты соответствующие договоренности на региональном уровне и на различных тематическиз форумах, которые затем послужат основанием для выработки договренностей на глобальном уровне. При этом предполагается, что все заинересованные международные организации должны принимать участия в этом процессе.

Помимо военно-политического измерения проблемы международной информационной безопасности Россия уделяет большое внимание противодействию информационному терроризму и информационной преступности. В мае 2017 г. Россия представила проект универсальной конвенции ООН о сотрудничестве в сфере противодействия информационной преступности для широкого обсуждения[524].

Внешняя политика России в отношении информационной безопасности и управления Интернетом определяется ее национальными интересами. Основной целью своей политики Россия видит формирования на глобальном уровне универсального международно-правового режима информационной безопасности,

[524] Ответ спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских на вопрос информагентства ТАСС о состоянии международного диалога в этой сфере // Официальный сайт МИД России. 29.06.2017. URL: http://www.mid.ru/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/2804288

который бы препятствовал использование данных новых технологий в военных и агрессивных целях.

В «Стратегии развития информационного общества в Российской Федерации» в качестве приоритетной цели была обозначена Интернационализация контроля над Интернетом. В 2010 г. Россия направила своего представителя в ICANN в подразделение, в котором вырабатывается политика в отношении странового уровня доменов. Это решение было вызвано необходимостью обеспечить представительство интересов России в ключевых институтах управления Интернетом. Кроме этого, в состав Правительственного консультативного комитета ICANN в 2009 г. были введены представители Министерство связи и массовых коммуникаций Российской Федерации. В результате, согласно России, ICANN становится подотчетной не только одному правительству США, но и всем правительствам, представители которых входят в консультативный комитет.

Обсуждение вопросов развития Интернета в России идет уже давно, при участии всех заинтересованных сторон. Так, Российский Интернет Форум (РИФ), ведущая ежегодная конференция Рунета проводится с 1997 г. В 2010 г. в Москве прошел первый Российский форум по вопросам управления Интернетом. Впоследствии аналогичные форумы проводились ежегодно. Форум 2012 г. был посвящен проблемам информационной безопасности. В ходе пятого российского форума по управлению Интернетом в 2014 г. проблема кибербезопасности была выделена в отдельную панель для обсуждения наряду с вопросами интернационализации управления Интернетом, защиты детей в Интернете, электронного правительства и экономики доменной индустрии[525].

В основе позиции России лежат основные принципы международного права, а именно уважение государственного суверенитета, недопущение агрессии, необходимость мирного разрешения международных споров. Указанные принципы применительно к глобальному информационному пространству

[525] Программа Четвёртого российского форума по управлению Интернетом. Москва, 25 апреля 2013 г. // Российский форум по управлению Интернетом: официальный сайт. URL:http://rigf.ru/prog/

отчасти уже нашли свое закрепление в международно-правовых документах: в ежегодно Резолюции ГА ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», в документах Всемирной встречи на высшем уровне по вопросам информационного общества; в итоговых документах саммитов БРИКС, в официальных документах ШОС, ОДКБ и СНГ.

Россия выступает за формирование безопасного глобального и регионального информационного пространства, с целью недопущения массированного распространения недостоверной или заведомо ложной социально-политической информации, способной нарушить общественную стабильность, как в отдельных государствах, так и на международном уровне; а также недопущение милитаризации информационного пространства.

В соответствии с российской позицией, недопущение использования Интернета в военно-политических целях необходимо рассматривать в рамках более широкой триады угроз международной информационной безопасности (военно-политическая угроза, информационная преступность и информационный терроризм) и продолжать работу в рамках уже задействованных на данном направлении организаций и принятых документов. Россия неоднократно заявляла, что она полностью поддерживает принцип, в соответствии с которым «ни одно правительство не должно обладать преимущественными полномочиями в вопросах международного управления Интернетом»[526].

Охлаждение в отношениях с США, странами ЕС и другими государствами Запада, связанное с воссоединением с Крымом, повлекли за собой отказ от ряда достигнутых договоренностей в сфере информационной безопасности. Но все же сохраняются каналы для взаимодействия, позволяющие разрешать вопросы, представляющие взаимный интерес. Так, в 2014 году начала работу Группа правительственных экспертов ООН, которая обсуждает вопросы применимости

[526]Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/4-R. Декларация принципов. Построение информационного общества – глобальная задача в новом тысячелетии – Женева, 2003. URL:http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-R.pdf

международного права к информационной сфере. В условиях общего похолодания в отношениях с Западом активизируется взаимодействие с азиатскими странами. Традиционно, позиции России и Китая в области международной информационной безопасности во многом совпадали. В последние месяцы также развивается взаимодействие с КНР по вопросам создания защищенной и устойчивой инфраструктуры национальных сегментов Сети.

Проведенный в настоящей работе анализ позволяет сформулировать ряд рекомендаций российской внешней политике в сфере информационной безопасности и управления Интернетом.

1. Россия заинтересована в принятии международно-правовых документов в области информационной безопасности, однако на современном этапе формирование всеобъемлющего режима информационной безопасности (в широкой трактовке термина) представляется труднодостижимой задачей. Несмотря на очевидную сдержанность в данном вопросе представителей США и ряда других развитых стран, Россия может получить поддержку таких государств как Китай, Бразилия, Саудовская Аравия и др. Нельзя не согласиться с предложениями российских исследователей А.В. Федорова и А.В. Крутских, которые полагают, что в качестве основы подобного документа следует использовать подходы, изложенные в российском проекте «Принципов международной информационной безопасности»[527]. Стоит отметить, при обсуждении вопроса информационной безопасности российские специалисты отдают приоритет противодействию вмешательству во внутренние дела страны, а также защите военных и финансовых структур. При этом масштабы промышленного шпионажа и ущерба, нанесенного экономике, остаются недооцененными. Представляется целесообразным включить данную проблематику в повестку дня международных переговоров. Более того, на современном этапе возможно более эффективным было бы обсуждение

[527]Технологический прогресс и современные международные отношения / под общ.ред. А.В. Крутских — М.: Просвещение, 2004.; Федоров А.В. Информационная безопасность в мировом политическом процессе: учеб. пособие. – М.: МГИМО(У), 2006.

возможности сотрудничества и достижения компромиссов в отдельных сферах информационной безопасности (в частности, по вопросам международного сотрудничества в области защиты информационных инфраструктур), что впоследствии могло бы послужить основой для договоренностей по более общим вопросам. Целесообразным также является обсуждение возможностей международно-правового закрепления основных направлений сотрудничества на техническом уровне, между CERT (Computer Emergency Response Team) различных государств.

2. Вопросам международного управления Интернетом в российской внешней политике уделяется в последние годы все больше внимания, прежде всего, в контексте обеспечения международной информационной безопасности. Положения, затрагивающие проблему управления Интернетом на международном уровне, представлены в Стратегии развития информационного общества, Концепции внешней политики и Доктрине информационной безопасности, а также в ряде документов, разработанных МИД России и представленных международным организациям и форумами.

Однако, как представляется, данная проблема заслуживает более пристального внимания. Специальный программный документ, посвященный проблематике управлением Интернетом, развивающий положения уже существующих документов, мог бы четко обозначить приоритеты российской внешней политики в данной сфере. За основу можно взять положения, характеризующие позицию России в ходе Всемирной встречи на высшем уровне по вопросам информационного общества и Форума по вопросам управления использованием Интернета, которая заключается в признании необходимости интернационализации управления Интернетом, обеспечения информационной безопасности и создания условий для развития многоязычия, а также использования Интернета в целях развития. Это позволит скоординировать политику различных российских ведомств, участвующих в выработке нашей позиции по этим вопросам, таких как Министерство связи и массовых коммуникаций, Министерство иностранных дел, Совет безопасности и др.

3. Россия объективно заинтересована в создании единого международно-правового режима, регулирующего деятельность государств в глобальном информационном пространстве в целях обеспечения международной информационной безопасности. Формирование подобного режима затрудняет тот факт, что информационное пространство, ключевой инфраструктурой которого является глобальная сеть Интернет, – это технология, затрагивающая чувствительные интересы большинства государств мира, в особенности развитых стран. Однако, у международного сообщества уже есть опыт международного взаимодействия в чувствительных с точки зрения национальных интересов и безопасности областях, в частности, можно опираться на опыт кодификации международного космического права, международный режим контроля над ядерными вооружениями. Целесообразно задействовать опыт МСЭ, поэтапно расширявшего сферу ответственности от телеграфного союза до взаимодействия в такой технологически сложной и значимой с точки зрения безопасности отрасли как электросвязь, поэтому важно подключение Союза к переговорному процессу и поддержка ее инициатив. Представляется также целесообразным создание Специального комитета ООН по управлению Интернетом (сходного с Комитетом ООН по космосу), который выступал бы в роли площадки для согласования интересов государств и выработки норм международно-правового регулирования в сфере управления интернетом и обеспечения информационной безопасности.

4. Для реализации Российской позиции важно продолжать активно использовать потенциал международных правительственных организаций, а именно активно участвовать в работе ООН, МСЭ, а также региональных организаций, в первую очередь СНГ и ШОС, и специализированных форумов, участвующих в обсуждении проблематики информационной безопасности и управления Интернетом.Принимая во внимание глобальный охват технологии, необходимо содействовать диалогу в рамках таких организаций, как ООН, МСЭ, ВОИС, как наиболее развитых институтов международного сотрудничества в глобальном масштабе, обладающих, кроме того, ресурсами правосубъектности и легитимности. При этом следует помнить, что сторона - инициатор заключения

тех или иных договоренностей может приобрести существенное преимущество и стараться сохранять инициативу.

Россия не является членом некоторых организаций, играющих значимую роль в формировании глобальных инструментов обеспечения международной информационной безопасности, – в частности, ОЭСР. В результате позиция России не учитывается в ходе принятия решений в рамках подобных организаций. В этих условиях важно интенсифицировать работу в рамках международных площадок с участием России с целью недопустить перехвата инициативы и принятия международных норм, не соответствующих национальным интересам страны.

Аналитики отмечают, что в сфере информационных технологий формируются новые альянсы[528]. Формирование и укрепление союзнических связей между государствами имеет место и в сфере информационной (и кибербезопасности) и управления Интернетом, причем в увязке с политико-экономическими аспектами глобальной информатизации. В качестве примера можно привести договоренности между США и ЕС соглашения Safe Harbour (Safe Harbour Privacy Priniples, Соглашение «Безопасная гавань» о принципах защиты персональной информации – рамочное соглашение между США и ЕС, а также США и Швейцарией, согласно которому Интернет- и ИТ компании, базирующиеся в США, но ведущие бизнес в странах ЕС, обрабатывают персональные данные пользователей в соответствии с принципами, закрепленными в Директиве ЕС 95/46/ЕС о защите персональных данных, а не законодательством США, которое является менее строгим в данном отношении. Таким образом, формируется относительно автономный международный режим защиты персональных данных в этих государствах). В интересах России интенсификация сотрудничества с государствами, разделяющими российское видение угроз и перспектив глобальной информатизации. Участники таких

[528]См. Технологический прогресс и современные международные отношения / под общ.ред. А. В. Крутских. М.: Просвещение, 2004. 446 с.; Федоров А.В. Информационная безопасность в мировом политическом процессе: учеб. пособие. М.: МГИМО, 2006. – 218 с.; Farell H. Constructing the International Foundations of E-Commerce: The EU - U.S. Safe Harbor Arrangement // International Organization. 2003. No 2(57). P. 277-306.

организаций, как СНГ, ОДКБ, ШОС и БРИКС также признают необходимость совместного регулирования Сети и развития сотрудничества в сфере информационной безопасности. Участники этих организаций имеют сходный уровень развития телекоммуникационной отрасли и информационных технологий, сходное восприятие угроз информационной безопасности, как на национальном, так и на международном уровнях. При этом, учитывая значимость политико-экономической проблематики, целесообразно было бы включить экономические проблемы (в частности, вопросы сотрудничества ИТ-компаний, допуска на рынки, обмена передовым опытом и технологиями) в повестку дня названных организаций.

5. Принимая во внимание растущую значимость многоуровневых форматов сотрудничества в сфере международного управления интернетом и обеспечения безопасности, в интересах России содействие участию российских организаций экспертного сообщества в обсуждении данных проблем.

В этой связи целесообразно способствовать усилению и развитию российского исследовательского сообщества в сфере ИКТ (в первую очередь путем грантовой, финансовой поддержки, развития вузовской подготовки соответствующих специалистов), но и активизировать сотрудничество с такими организациями, как ICANN, W3C, IETF: это позволит получить доступ к передовым знаниям и опыту, а также оказывать влияние на решения, принимаемые в рамках этих организаций. Кроме того, необходимо поддерживать участие российских представителей в работе таких площадок, как Форум по вопросам управления Интернетом.

6. «Как представляется, одним из наиболее перспективных направлений российской цифровой дипломатии является вовлечение технологического отечественного бизнеса в проекты в сфере публичной дипломатии. Первые шаги на данном направлении уже были сделаны. Успешен опыт поисковой компании Yandex, которая сегодня обрабатывает большую часть запросов русскоязычного Интернета, социальной сети «В контакте», популярной не только в России, но и во многих странах зарубежья, включая государства СНГ, Израиль, Германию и

США. В формирование позитивного образа российской политики и дипломатии весомый вклад вносят телеканалы «Первый канал» и RT (бывший Russia Today) вещающие также в цифровом пространстве. Уже созданы блоги российских государственных чиновников и дипломатов на русском и английском языках, на порталах государственных органов публикуются открытые данные об их деятельности. Вместе с тем компании Рунета могут быть более активно задействованы в российской цифровой дипломатии для популяризации русского языка и культуры, эффективного донесения российского видения международных проблем до глобальной аудитории.

Услуги компаний и сервисов российского сегмента глобальной сети пользуются популярностью у русскоязычного населения независимо от места проживания. Представляется целесообразным создание и продвижение этими компаниями инициатив, направленных на взаимодействие с зарубежными русскоязычными диаспорами, в том числе научными и профессиональными. Возможным вариантом такого взаимодействия могло бы стать создание специального информационного портала, который предоставлял бы актуальную информацию о возможностях сотрудничества русскоязычной научной диаспоры за рубежом с научными институтами в РФ, создавал бы прямые каналы коммуникации и способствовал решению организационных вопросов такого взаимодействия»[529].

Современные достижения развития ИКТ, в частности, появление информационного оружия, вирусов и пр., а также широкое использование социальных сетевых сервисов, уже не утратят своего значения по мере технологического развития. В этом контексте важно признать необходимость и неибежность. государственного участия в управлении и направлении их использованием и их влиянием на динамику общественного развития в соответствии с национальными интересами[530]. Политика России по обеспечению

[529]Зиновьева Е.С. Цифровая дипломатия, международная безопасность и возможности для России // Индекс безопасности. 2013. № 1. С. 216.
[530] См. напр: Lichtenstein J. Digital Diplomacy // New York Times Magazine.16.07.2010. URL:http://www.nytimes.com/2010/07/18/magazine/18web2-0-t.html?pagewanted=all

международной информационной безопасности и управлению интернетом, вероятно, будет также проводиться в русле осознания значимости новых тенденций технологического развития. Важно пытаться найти баланс между безопасностью и проактивной внешней политикой в информационном пространстве, направленной на укрепление мягкой силы и повышение привлекательности России. Необходимо вовлекать в задачи реализации внешнеполитических целей представителей частного сектора и гражданского общества при ведущей и координирующей роли государства. При этом обеспечение информационной безопасности на национальном и на международном уровнях остается обязанностью и прерогативой государства.

5. Сложилась благоприятная ситуация для продвижения российской инициативы по принятию международного документа в рамках ООН, направленного на борьбу с киберпреступностью. Страны Запада, прежде всего США, позиционируют Конвенцию о киберпреступности Совета Европы от 2001 г. как универсальный документы в данной области, действие которого может быть распространено на глобальный уровень. Однако для России использование данной конвенции представляется неприемлемым по причине ее ограничительного характера, так как согласно пункту “b” статьи 32 данной Концепции, сторона Конвенции может иметь через компьютерную систему на своей территории доступ к компьютерным данным, хранящимся вдругом государстве, тоже являющимся стороной Конвенции. Как отмечает А.И. Смирнов, «положения данного пункта на практике могут толковаться как предоставляющие право производства трансграничного обыска в компьютерных сетях без согласия заинтересованной стороны. Более того, применение данного положения может нанести ущерб национальной безопасности и суверенитету государства, что неприемлемо для России»[531].

Вместе с тем, конвенция была принята 14 лет назад, следовательно, отдельные ее положения существенно устарели, особенно принимая во внимание

[531]Глобальная безопасность: инновационные методы анализа конфликтов / под ред. А.И. Смирнова. М: Общество «Знание» России, 2011. С. 187

темпы развития ИКТ. В этой ситуации многие государства, прежде всего, страны БРИКС, разделяют предлагаемую Россией идею о разработке универсальной конвенции о борьбе с преступностью в сфере ИКТ в рамках ООН, которая основывалась бы на уважении суверенитета государств-участников и обеспечила бы эффективное сотрудничество по противодействиюкиберпреступности.

6. Вопрос защиты персональных данных пользователей сети Интернет логично вписывается в стратегию России по отношению к информационным угрозам. После появления инструментов, позволяющих обрабатывать «большие данные», бизнес и государство активно используют их в своих целях. В рамках социального инжиниринга «большие данные» могут быть применены для воздействия на широкую общественность и отдельные группы людей. В контексте программ цифровой дипломатии и потенциальных «цветных революций», существует опасность их использования для манипуляции общественным мнением и подрыва экономической, социальной, а также и политической стабильности в государстве. На сегодняшний день в ряде стран существуют правовые ограничения для бизнеса в использовании ИКТ для влияния на потребителей, но такого рода ограничения полностью отсутствуют в сфере международных отношений; более того, возможные действия государств в данной области пока остаются вне правового поля. Россия заинтересована во введенииподобных ограничений на международном уровне, в том числе как угрозы вмешательства во внутренние дела государств при помощи инструментов социальных медиа и технологий социальной инженерии. Подобные ограничения также могут быть основаны на необходимости защиты индивидуальных свобод и права на невмешательство в частную жизнь, будучи вписаны, таким образом, в правозащитную проблематику международного сотрудничества. Они соответствовали бы также букве Устава ООН, в частности, принципу уважения государственного суверенитета и невмешательства во внутренние дела.

7. Формирование Интернета вещей (см. главу 1) - перспективное направление развития, которое потенциально может дополнить переговорную повестку дня в области международной информационной безопасности. Угрозы, связанные с

Интернетом вещей, весьма значимы, учитывая, что в современном мире интернет вещей используется повсеместно, следовательно и вмешательство в эту технологию может иметь серьёзные последствия. Помимо террористических и преступных угроз, исходящих из Интернета вещей, существуют также угрозы связанные с суверенитетом и безопасностью страны. Информация, собранная с помощью Интернета вещей позволяет осуществлять наблюдение за жизнью граждан, функционированием правительств, предприятий, что открывает возможности для сбора «больших данных» и их манипулированием в целях социального инжиниринга. Кроме того, полученная информация может быть использована для выявления критических уязвимостей, манипуляции общественным мнением, что представляет собой угрозу национальной и международной безопасности. На национальном уровне, можно предложить внедрение в законодательство страны обязательство для компаний, предоставляющих объекты имеющие доступ в Интернет, иметь центр обработки персональных данных на территории России. На международном уровне, обеспечение безопасности данных, полученных в результате сбора информации в рамках «интернета вещей», может быть обеспечено посредством многоуровневого международного сотрудничества при участии государств, крупного бизнеса, работающего в данной области, и авторитетных и легитимных международных организаций (ООН, МСЭ, ЮНИДО).

Выводы по главе:

На данный момент можно констатировать отсутствие целостности в глобальном режиме информационной безопасности. Его можно характеризовать как бессистемную совокупность отдельных режимов и инициатив, сформировавшихся вокруг ответов на различные вызовы информационной безопасности.

Международное сотрудничество на глобальном уровне по обеспечению информационной безопасности сегодня пребывает на этапе определения повестки дня. Особенностью данного этапа, согласно теории международных режимов, является взаимодействие международных неправительственных организаций и научных центров, благодаря которому формируются эпистемичнские сообщества способные оказывать активное влияние на определение повестки дня. Необходимо отметить, что наблюдаемые сегодня два секъюритизирущие дискурса и сформировавшие вокруг них различные эпистемические сообщества пока не сближаются.

Стадия определения повестки дня, согласно теории, сменяется переговорным процессом, который в свою очередь переходит уже непосредственно к реализации достигнутых на предыдущем этапе соглашений. Эти переходы возможны только в том случае, если стороны осознали баланс угроз и видят необходимость в выработке общих соглашений и их имплементации. Как правило, такое осознание приходит, к сожалению, только после острых международных кризисов. Иначе стороны будут бесконечно долго задерживаться на первой стадии или на второй. В сфере международной информационной безопасности такого кризиса пока не произошло, кроме того на восприятие угроз влияети и специфика информационного и кибер оружия, которая заключается в сложности определения источника удара, а также в асимметрии наступательных и оборонительных потенциалов. Пока возможности наступательного оружия существенно превышают потенциал оборонительного.

При этом необходимо отметить, что задержка первого этапе – это средний показатель глобального режима информационной безопасности. В ряде регионов стороны уже перешли не только к переговорной стадии, но и к имплементации достигнутых договорённостей. Такими регионами являются: Евроатлантика с институциональным зонтиком в форме НАТО, Юго-восточная Азия с институциональной привязкой к АСЕАН и Евразия, понимаемая как пространство ОДКБ и ШОС. Подобную ситуацию можно наблюдать в некоторых случаях на

двустороннем уровне. Здесь скорость перехода от стадии к стадии зависит от степени взаимного восприятия сторонами друг друга или третьей стороны в качестве угрозы, что определяются реальным наличием у сторон соответствующих военных потенциалов в информационной и кибер сфере. Зачастую, такие двусторонние режимы направлены на развитие доверия и предсказуемости в отношениях сторон.

Соединенные Штаты остается доминирующей политической силой в мире. Свое лидерство они стремятся обеспечить как в деле управления Интернетом, так и в сфере информационной безопасности. Исходя из этой цели, США не заинтересованы связывать себя договорными обязательствами в деле развития и военного использования ИКТ, особенно информационного оружия. С другой стороны, Вашингтон активно пропагандирует необходимость адаптирования старых и выработки новых международного гуманитарного права к информационной среде, что введет киберконфликты в нормативное поле, а, следовательно, легитимирует их. При этом следует помнить, что технологическое лидерство США не гарантировано и распространение новых технологий может его в любой момент подорвать.

Международное сотрудничество в сфере информационной безопасности скорее всего будет соответствовать общей логике развития международных отношений, которые сегодня развиваются в новых формах взаимодействия государств и негосударственных акторов, таких как многосторонние партнерства и многуровневое сотрудничество. Именно такие формы взаимодействия будут играть все большую роль в сфере международной информационной безопансости. При этом государства в них сохраняют ведущую, координирующую роль. Интересы России подталкивают ее поддерживать регионализпцию режима информационной безопасности. В частности, реализуя координирующую роль, Россия может выстроить режим информационной безопасности на евразийском пространстве вокруг институциональных центров таких организаций как ОДКБ и ШОС.

Поддержание регионализации режима информационной безопасности повышает возможности России влиять на региональный порядок в информационной сфере, который складывается на постсоветском пространстве. Это в частности позволяет снизить угрозы «цветных революций», которые зачастую распространяются как раз по информационным каналам социльных сетей и социальных медиа. Участвуя в формировании данного регионального режима, Россия вполне может использовать такие влиятельные новые технологии как «Большие данные» и «Интернет вещей» при обпределении повестки дня. Кроме того, ранее участие в строительстве режима создает преимущества «первопроходца».

ЗАКЛЮЧЕНИЕ

Развитие ИКТ, неотъемлеимой части современного научно-технологического развития, оказывает существенное влияние на международные отношения и мировую политику, способсвуя появлению новых вопросов на международной повестке дня, в том числе, связанных с обеспечением международной информационной безопасности. Д. Най приходит к следующему выводу: «В мире, основанном на информации, распыление власти может представлять более серьезную опасность, чем смена власти. Согласно традиционным представлениям, доминирует государство с наибольшей армией, но в век информации может победить тот, кто способен представить себя в лучшем свете»[532]. Современный этап информационной революции способствует распространению сетевых форм организации в мировой политике, изменению структуры международной системы, формированию многополярности, но и усилению негосударственных акторов.

При этом характеристики международной системы, в свою очередь, влияют на современное глобальное информационное пространство, в частности, рост конфликтности и тенденция к регионализации[533], оказывает влияние на характеристики глобального информационного пространства.

Обеспечение информационной безопасности становится одной из ключевых современных международных проблем в результате повсеместного использования и высокой зависимости от современных ИКТ. Значимость данной проблематики подтверждается высоким вниманием к ней в СМИ и внешней политике государств. Основная угроза международной информационной безопасности – это

[532]Най-мл. Д. Будущее американской власти // Россия в глобальной политике. 2010. № 6. URL:http://www.globalaffairs.ru/number/Buduschee-amerikanskoi-vlasti-15053

[533]См. напр.: Воскресенский А.Д. Структурирование регионального пространства и его основные акторы. Регионализация и трансрегиональное сотрудничество / А.Д. Воскресенский, Е.В. Колдунова, А.А. Киреева // Мировое комплексное регионоведение / Под ред. А.Д. Воскресенского. М.: Магистр-Инфра-М, 2014. – с. 80-107

возможность нарушения стабильности всей международной системы в условиях отсутствия всеобъемлющих договоренностей в данной области.

«Международная информационная безопасность трактуется, прежде всего, исходя из характера угроз. Традиционно выделялась «триада угроз» международной информационной безопасности — использование ИКТ в террористических, преступных и военно-политических целях (под военно-политическими целями понимается использование ИКТ в межгосударственных конфликтах). В частности, подобный подход к определению угроз был закреплен в ряде резолюций ГА ООН, посвященных проблематике информационной безопасности»[534].

Несмотря на значимость террористической и преступной угроз, важнейшей угрозой международной информационной безопасности является использование ИКТ государствами в военно-политических целях. Можно согласиться с отечественным экспертом А.В. Федоровым, который полагает, что «в результате распространения информационно-коммуникационных технологий изменяется характер социума, следовательно, изменяется характер возникающих в нем противоречий и их разрешения»[535]. Информационное воздействие становится неотъемлемой частью современных «гибридных войн» и межгосударственной конкуренции в мирное время. На международном уровне наметилась гонка информационных и кибер- вооружений.

В рамках информационно-технического измерения международной информационной безопасности особую опасность представляют угрозы критической информационной инфраструктуре государства, что может создать реальную угрозу национальной и международной безопасности не только в виртуальном, но и в реальном мире.

В рамках социо-гуманитарного измерения международной информационной безопасности актуализируется дискурс о возможном

[534]Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности // Право и управление. XXIвек. 2014. № 4. С. 45.
[535]Федоров А.В. Информационная безопасность в мировом политическом процессе. – М.: МГИМО(У), 2008. – 218 с.

использовании социальных медиа как каналов информационного воздействия. Таким образом, возрастающая зависимость всех сфер общества от электронных коммуникаций и Интернета ведет к тому, что манипуляция социальными сетями позволяет использовать уязвимости национальной и международной безопасности, усиливающиеся вследствие процессов глобальной информатизации.

Вместе с тем, глобальное информационное пространство как объект международного сотрудничества в целях обеспечения его безопасного использования и развития характеризуется рядом особенностей, отличающих его от иных областей, в частности:

- транснграничный характер информационного пространства и взаимозависимость государств в данной сфере усиливают уязвимость государств и негосударственных акторов;

- влияние негосударственных участников и неправительственных акторов в информационной сфере выше, чем в большинстве других областей мировой политики;

- объекты критической информационной инфраструктуры гражданского и военного назначения тесно связаны между собой, большая же часть критической информационной инфраструктуры может быть отнесена к объектам двойного назначения. В этой связи в ходе информационной войны зачастую невозможно провести различие между гражданскими и военными целями, что осложняет применимость существующего корпуса международного гуманитарного права;

- анонимность и повсеместный характер использования ИКТ осложняет идентификацию источника информационного воздействия, которое может быть замаскировано под системную ошибку, что в свою очередь затрудняет оценку масштаба ущерба, меру ответного удара, а также применение традиционных в международных отношениях механизмов сдерживания.

Эта специфика определяет характеристики механизмов международного сотрудничества в данной области. Международное сотрудничество по обеспечению информационной безопасности наталкивается на противоречия в

государственных интересах. Одним из ключевых факторов являются противоречивые взгляды на проблему информационной безопасности, предлагаемые США и странами Запада, с одной стороны, и Россией, Китаем и странами развивающегося мира – с другой[536]. Если Китай, Россия и развивающиеся страны поддерживают необходимость государственного участия в регулировании информационной сферы и международно-правовую регламентацию проблематики обеспечения информационной безопасности, то США предпочитают частную модель регулирования.

Однако в последние годы наметилось изменение баланса сил в глобальном информационном пространстве. В США приходит осознание того, что наиболее развитое в сфере ИКТ государство оказывается самым уязвимым. Следствием этого является изменение позиции относительно международно-правового регулирования информационной сферы. США в последние годы более склонны поддерживать многосторонние инициативы по обеспечению информацинной безопасности (в американской терминологии «кибербезопасности»), что открывает возможности для развития сотрудничества, формирования глобального режима в данной сфере.

Типологически международное сотрудничество по обеспечению информационной безопасности не существенно отличается от моделей международного взаимодействия, сложившихся в рамках других высокотехнологичных областей мировой политики, что было обозначено как «технологический изоморфизм» в мировой политике. При этом «технологический изоморфизм» не абсолютен, следует отметить также и различия, связанные со спецификой технологий, особенностями восприятия угроз, порождаемых их потенциальным использованием в военных целях, а также характеристиками международной системы.

[536]Lieberthal K., Singer P. Cybersecurity and U.S. – China Relations // Jonh L. Torton China Institute in Brookings. 2012. URL:http://www.brookings.edu/~/media/Research/Files/Papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.PDF

Гипотеза исследования подтвердилась – ввиду высокой значимости информационной безопасности и отсутствия баланса угроз (на что влияет, в том числе и специфика ИКТ) международное сотрудничество находится на глобальном уровне на этапе переговоров, что маскирует гонку вооружений, и пока не перешло на этап реализации достигнутых соглашений. «На современном этапе не сложилось единого глобального режима обеспечения информационной безопасности. Скорее, мы можем наблюдать совокупность разрозненных инициатив и режимов, направленных на решение специфических проблем безопасности, возникающих в «цифровую эпоху», что в определённой степени отражает тенденцию регионализации в мировой политике и информационном пространстве.

В ряде регионов сложились эффективные режимы информационной безопасности, сторонам удалось выработать повестку дня, договориться по согласованным вопросам и приступить к имплементации достигнутых решений: Евроатлантический регион в рамках НАТО, Юго-восточная Азия в рамках АСЕАН, евразийский регион в рамках ОДКБ и ШОС. На двустороннем уровне сотрудничество по вопросам информационной безопасности реализуется, как правило, между государствами, обладающими значительными киберпотенциалами (и воспринимающими друг друга как угрозу или же объединяющимися против общей угрозы) и режимы двустороннего взаимодействия находится в состоянии имплементации»[537].

Можно предположить, что в краткосрочной перспективе глобальный режим информационной безопасности будет развиваться по аналогии с международно-правовым режимом космического пространства, что обусловлено схожестью условий (неэффективностью оборонительных стратегий, общей уязвимостью, стремлением государств сохранить «свободу рук» в отношении военного использования новых перспективных технологий) и будет использовать в

[537]Зиновьева Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности // Вестник МГИМО – Университета. 2016. № 4. С. 237.

основном инструменты «мягкого права». Однако, двусторонние договоренности о мерах доверия (между США и Россией, США и Китаем и др.) и растущая технологическая сложность информационного оружия и, как следствие, его труднодоступность для большинства государств, в долгосрочной перспективе могут привести к формированию более «жесткого» международного режима, во многом схожего с режимом нераспространения ядерного оружия, ориентированного на закрепление привилегированного положения великих держав.

Международное сотрудничество по обеспечению информационной безопасности, так же как и управлению, Интернетом, не может быть эффективным без привлечения негосударственных акторов, которые обладают необходимыми ресурсами и экспертизой, а также могут выступать в качестве участников определения повестки дня и имплементации сложившихся договоренностей. Можно утверждать, что распространенность моделей многоуровневого взаимодействия при обеспечении информационной безопасности на глобальном и региональных уровнях будет возрастать. При этом за государствами сохранится ведущая и координирующая роль в ходе международного взаимодействия.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Источники

Официальные документы Российской Федерации

1. Доктрина информационной безопасности Российской Федерации. Утверждена указом Президента № 646 от 5.12.2016. URL: http://www.scrf.gov.ru/documents/6/5.html
2. Доктрина информационной безопасности Российской Федерации. Утверждена указом Президента 09.09.2000. Пр-1895. URL:http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm
3. О некоторых вопросах информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 22.05.2015 № 260. URL: http://www.rg.ru/2015/05/26/rosset-dok.html
4. Конвенция об обеспечении международной информационной безопасности (концепция). Утвеждена 22.09.2011. URL:http://mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument
5. Концепция внешней политики Российской Федерации. Утверждена 30.11.2016. URL:http://www.scrf.gov.ru/documents/2/25.html
6. О безопасности: закон РФ (с изменениями 02.03.2007) . Утвержден 05.03.1992. N 2446-I
7. О Федеральной целевой программе "Электронная Россия (2002-2010 годы)": постановление Правительства РФ N 65 от 28.12.2002. URL:http://www.internet-law.ru/intlaw/laws/e-rus.htm
8. О государственной программе Российской Федерации "Информационное общество (2011-2020 годы): распоряжение Правительства Российской Федерации от 20.10.2010. № 1815-р // Российская газета. 16.11.2010. URL:http://www.rg.ru/2010/11/16/infobschestvo-site-dok.html

9. Стратегия национальной безопасности Российской Федерации до 2020 года: указ Президента № 537. Утверждена 12.05.2009. URL:http://www.mid.ru/ns-osndoc.nsf/0e9272befa34209743256c630042d1aa/8abb3c17eb3d2626c32575b500320ae4?OpenDocument

10. Стратегия развития информационного общества в Российской Федерации. Утверждена 7.02.2008. Пр-212. URL:http://www.mid.ru/ns-osndoc.nsf/0e9272befa34209743256c630042d1aa/453f799b9fe0637cc32573f3002b2558?OpenDocument

11. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. Утвержденауказом Президента 09.05.2017. № 203. URL: http://kremlin.ru/acts/bank/41919

12. Об информации, информационных технологиях и о защите информации: Федеральный закон РФ от 14.07.2006. URL:http://www.minkomsvjaz.ru/ministry/documents/768/2745.shtml

13. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: указ Президента Российской Федерации № 351 от 17.03.2008. URL:http://www.businesspravo.ru/Docum/DocumShow_DocumID_135839.html

14. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Утв. Президентом Российской Федерации Пр. № 1753 от 01.08.2013. / Совет Безопасности РФ. URL:http://www.scrf.gov.ru/documents/6/114.html

15. Военная доктрина Российской Федерации. Утв. Президентом РФ 25.12.2014. Пр-2976. URL: http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/2a959a74cd7ed01f432569fb004872a3!OpenDocument

16. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации». Проект. URL: regulation.gov.ru/get.php?view_id=3&doc_id=12366

17. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" N 187-ФЗ 26.07.2016. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/
18. О государственной программе Российской Федерации "Информационное общество (2011-2020 годы): распоряжение Правительства Российской Федерации от 20 октября 2010 г. № 1815-р // Российская газета. 16.11.2010. URL:http://www.rg.ru/2010/11/16/infobschestvo-site-dok.html

Официальные документы США

19. Critical Infrastructure Protection: Executive Order 13010 // Federal Register. July 17, 1996. Vol. 61, No. 138
20. White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive No.63
21. Establishing the Office of Homeland Security and the Homeland Security Council: Executive Order 13228 // Federal Register, Vol. 66, No. 196. October 8, 2001.
22. The National Strategy for Homeland Security: U.S. Department of Homeland Security. July 16, 2002.
23. The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets: White House, Executive Office of the President. February, 2003.
24. Homeland Security: Presidential Directive 7, HSPD-7. December, 2003.
25. IT Strategic Plan. Digital Diplomacy: Fiscal Years 2011-2013 // US Department of State. September 1, 2010. URL:http://www.state.gov/m/irm/rls/148572.htm
26. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001: H.R. 3162.
27. The Department of Defense Cyber Strategy. Washington, April, 2015. URL: http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
28. Executive Order 13694 Blocking the Property of Certain Persons Engaging in Significant

Malicious Cyber-Enabled Activities. Washington, April, 2015. URL: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf

Официальные документы Китайской народной республики

29. International Strategy of Cooperation on Cyberspace. Ministry of Foreign Affairs of the People's Republic of China, 01.03.2017. URL: http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm

Документы и источники международных правительственных организаций и форумов

Организация Объединенных Наций

30. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора. Группа экспертов для проведения всестороннего исследования киберпреступности Вена, 25-28 февраля 2013 года. UNODC/CCPCJ/EG.4/2013/2 URL: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf

31. Декларация правовых принципов, регулирующих деятельность государств по исследованию и использованию космического пространства. Резолюция ГА ООН 1962 (XVIII). Нью-Йорк, 13.12.1963. URL: http://www.un.org/ru/documents/decl_conv/declarations/outerspace_principles.shtml

32. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: Исследование 33 // Управление по вопросам разоружения. ООН, Нью-Йорк, 2012.

33. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/RES/63/37. 02.12.2008.

34. Определение агрессии. Утв. резолюцией 3314 (XXIX) ГА ООН. Нью-Йорк, 14.12.1974. URL: http://www.un.org/ru/documents/decl_conv/conventions/aggression.shtml

35. Правила поведения в области обеспечения международнойинформационной безопасности: письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 г. на имя Генерального секретаря. A/66/359.

36. Правила поведения в области обеспечения международнойинформационной безопасности: письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 г. на имя Генерального секретаря. A/66/359.

37. Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур // Резолюция, принятая Генеральной Ассамблеей 21 декабря 2009 года. A/RES/64/211. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/474/51/PDF/N0947451.pdf?OpenElement

38. General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/65/201, 30 July 2010.

39. UN Bangkok Declaration. Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice. A/CONF.203/L.5. Bangkok, 2005.

40. UN Electronic Commerce Agreement (Recommendation No31). ECE/TRADE/257. Geneva, 2000. URL:http://www.unece.org/cefact/recommendations/rec31/rec31_ecetrd257e.pdf

41. UNCITRAL Model Law on Electronic Commerce 1996 with Additional Article 5 bis (1998) and Guide to Enactment. A/51/628 New York, 2006.

ЮНЕСКО

42. Итоговый документ международной конференции “ЮНЕСКО между двумя этапами Всемирного саммита по информационному обществу” Санкт-Петербург, 2005 г. URL:http://confifap.cpic.ru/conf2005/rus/info/str_166.html

43. Рекомендация о развитии и использовании многоязычия и всеобщем доступе к киберпространству. ЮНЕСКО. Париж, 2003. URL: http://www.ifap.ru/ofdocs/multcybe.rtf

44. UNESCO Position Statement on Internet Governance. Shato de Bossy 2004. URL:www.ifap.ru/projects/wgig01.doc

Всемирная организация интеллектуальной собственности

45. Общий отчет Ассамблеи государств – членов ВОИС. Тридцать седьмая серия заседаний. A/37/14. Женева, 2002. URL: http://www.wipo.int/edocs/mdocs/govbody/ru/a_37/a_37_14.doc

46. Final Report of the WIPO Internet Domain Name Process. — Geneva, 1999. URL:http://www.wipo.int/export/sites/www/amc/en/docs/report-final1.doc

47. World Intellectual Property Organization Copyright Treaty // S. TREATY DOC. NO. 105-17, 36 I.L.M. 65. – Geneva, 1996.

48. World Intellectual Property Organization Performances and Phonograms Treaty // S. TREATY DOC. NO. 105-17, 36 I.L.M. 76 – Geneva, 1996.

Международный союз электросвязи

49. Всемирная ассамблея по стандартизации электросвязи МСЭ ВАСЭ-08 − Резолюция 50 — Йоханнесбург, 2008. URL:http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-R.pdf

50. ITU World Information Society Report. Geneva, 2006. URL: http://www.itu.int/osg/spu/publications/worldinformationsociety/2006/wisr-web.pdf

51. World Telecommunication and Standartization Assembly Resolution. IP Address allocation and encouragement of the deployment of IPv6. – Johannesburg, 2008. URL: http://www.itu.int/publ/T-RES-T.64-2008/en

52. World Telecommunication and Standartization Assembly Resolution. Non-discriminatory access and use of Internet resources. – Johannesburg, 2008. URL: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.69-2008-PDF-E.pdf

Всемирная торговая организация

53. Doha WTO Ministerial Declaration WT/MIN(01)/DEC/1 Doha, 2001. URL:http://www.wto.org/english/thewto_e/minist_e/min01_e/mindecl_e.htmNoelectronic

54. WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) Marrakesh, 1994. URL:http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm

55. WTO Declaration on Global Electronic Commerce. Geneva, 1998. URL: http://www.wto.org/anniv/ecom.htm

56. WTO Work programme on electronic commerce. Adopted by the General Council on 25.09.1998 // WTO: official site. URL:http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm

Организация экономического сотрудничества и развития

57. OECD "Internet Content Self-Regulation Dialogue". Member Statement on "Impact of Self-Regulation and Filtering on Human Rights to Freedom of Expression" Paris, 1998. URL:http://www.gilc.org/speech/ratings/gilc-oecd-398.html

58. OECD Work Plan of the WP9 Sub-Group on Electronic Commerce 2001-2003. // Official site of the OECD. URL:http://www.oecd.org/document/46/0,3343,en_2649_33741_1834414_1_1_1_1,00.html

59. OECD Working Party on Telecommunication and Information Services Policies. Internet Traffic Prioritization: an Overview. DSTI/ICCP/TISP(2006)4/FINAL. URL:http://www.oecd.org/dataoecd/43/63/38405781.pdf

«Группа семи»

60. Итоговое заявление председателя саммита «Группы семи» в Санкт-Петербурге. Санкт-Петербург, 2006. URL: http://g8russia.ru/docs/25.html

61. Довильская декларация «Группы семи»: «Неизменная приверженность свободе и демократии». Довиль, 2011. URL: http://kremlin.ru/supplement/946

62. Окинавская Хартия глобального информационного общества. -- Окинава, 2000.
URL: http://www.ifap.ru/ofdocs/okinhar.htm

63. The Evian summit G8 chair's summary. Evian, 2003.
URL:http://www.g8.fr/evian/english/navigation/2003_g8_summit/summit_documents/chairs_summary.html

64. The Kananaskis Summit G8 Chair's Summary. Kananaskis, 2002.
URL: http://www.g8.gc.ca/2002Kananaskis/chairsummary-en.asp

65. G8 Background paper: International action against Cybercrime.
URL: http://www.diplomatie.gouv.fr/actual/evenements/cybercrim/fiche3.gb.html

Совет Европы

66. Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. ETS No: 185. Strasbourg, 1981.
URL:http://www.legislationline.org/legislation.php?tid=219&lid=6134&less=false

67. Council of Europe Convention on cybercrime. ETSNo: 108. — Budapest, 2001.
URL:http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Европейский союз

68. Директива ЕС 2006/24/ЕС о сохранении информации, созданной или обработанной в связи с оказанием услуг связи, и внесении изменений в Директиву ЕС о защите персональных данных.

69. Концепция развития информационного общества Европейского союза. 11.05.07.
URL: www.soi.ru/soi/85735,

70. Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union. 6.07.2016. URL: http://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

71. Regulation No 733/2002 of the European Parliament and of the Council on the implementation of the .eu Top Level Domain. ITRE/5/14954. Strasburg, 2002.
72. Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. COM(2013) European Commission. Brussels, 7.02.2013 URL: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
73. Cyber Security strategy of the European Union: An open, safe and secure Cyberspace. JOIN (2013). European Commission. Brussels, 7.02.2013. URL: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
74. European Union Action Plan on Promoting Safer Use of the Internet. 276/1999/EC.
URL: http://europa.eu.int/ISPO/iap/decision/en.html

Содружество Независимых Государств

75. Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. Минск, 2001. URL:http://www.gipi.kg/rus/readarticle.php?article_id=131
76. Итоговый документ международного семинара СНГ «Управление использованием Интернета». Кишинев, 2005. URL:http://www.rcc.org.ru/ru/news/documents/2005-01.doc
77. Проект модельного закона СНГ «Об Интернете» / Межпарламентская ассамблея государств-участников СНГ. 2007.
URL:http://www.raecs.ru/files/modelnyi_zakon_sng_po_intrnetu.pdf

Шанхайская организация сотрудничества

78. Душанбинская декларация от 28.08.2008. URL: http://infoshos.ru/ru/?id=39

79. Бишкекская декларация от 16.08.2007. URL: http://infoshos.ru/ru/?id=25

80. Совместная декларация КНР и РФ от 26.02.2007. URL:http://www.fmprc.gov.cn/rus/wjdt/gb/t307521.htm

81. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2009 г. // Международная информационная безопасность: дипломатия мира: сборник материалов / под ред. С.А. Комова. М., 2009.

Азиатско-Тихоокеанская организация экономического сотрудничества

82. Shanghai Declaration. Statement on the Security of Information and Communications Infrastructures. The Fifth APEC Ministerial Meeting on Telecommunications and Information Industry. TELMIN5/1. Shanghai, 2002. URL:http://www.apec.org/apec/documents_reports/telecommunications_information_ministerial_meetings/2002.html

83. Chair's Report of the Telecommunications and Information Working Group to the Sixth APEC Ministerial Meeting on the Information Industry. 2005/TELMIN/002. Lima, 2005. URL:http://www.apec.org/apec/documents_reports/telecommunications_information_ministerial_meetings/2005.html

БРИКС

84. Форталезская декларация (принята по итогам шестого саммита БРИКС) Форталеза, 15.08. 2014 URL: http://static.kremlin.ru/media/events/files/41d4f1dd6741763252a8.pdf

ОБСЕ

85. PC.DEC/1202. Решение № 1202. Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования

информационных и коммуникационных технологий. 10.03.2016. URL: http://www.osce.org/ru/pc/228521?download=true

86. PC.DEC/1106. Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий. 3.12. 2013. URL: http://www.osce.org/ru/pc/109648?download=true

Документы и источники международных встреч и конференций

Всемирная встреча на высшем уровне по вопросам информационного общества

87. Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/5-R. План действий. — 12 декабря 2003 года.
URL: http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-R.pdf

88. Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/7-R. Тунисское обязательство. — 18 ноября 2005 года.
URL: http://www.itu.int/wsis/docs2/tunis/off/7-ru.pdf

89. Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R. Тунисская программа для информационного общества. — 18 ноября 2005 года. URL: http://www.itu.int/wsis/docs2/tunis/off/6rev1-ru.pdf

90. Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/4-R. Декларация принципов.

91. Доклад рабочей группы по управлению Интернетом. — Шато де Босси, 2005.
URL: http://www.wgig.org/docs/WGIGReport-Russian.pdf

92. Shaping Information Societies for Human Needs. Civil Society Declaration to the World Summit on the Information Society // WSIS Civil Society Plenary. – Geneva, 2003.

Форум по вопросам управления использованием Интернета

93. Форум по вопросам управления использованием Интернета. Обобщающий документ. — Хайдарабад, 2008. URL: http://www.ifap.ru/pr/2008/n081201a.pdf

94. Second Meeting of the Internet Governance Forum. Chairman's Summary. — Rio de Janeiro, 2007. URL: http://www.ictparliament.org/index.php/component/content/article/317-igf-2007-chairmans-summary-is-now-available

Женевские и Гаагские конференции

95. Дополнительный протокол I к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооруженных конфликтов (Протокол I). Женева, 8 июня 1977 г.

96. Второй протокол к Гаагской конвенции о защите культурных ценностей в случае вооруженного конфликта 1954 года. Гаага, 26 марта 1999 г.

Документы и источники международных неправительственных организаций

ICANN

97. Ответственность и прозрачность ICANN: структура и принципы // Принципы управления ICANN. — 2007. URL: http://www.icann.org/en/transparency/acct-trans-frameworks-principles-russian-17oct07.pdf

98. Contract Between ICANN and the United States Government for Performance of the IANA Function. — 1998. URL: http://www.icann.org/en/general/iana-contract-09feb00.htm

99. Memorandum of Understanding Between the Department of Commerce and the Internet Corporation for Assigned Names and Numbers. — 1998. URL: http://www.icann.org/en/general/icann-mou-25nov98.htm

100. Joint Project Agreement between the US Department of Commerce and the Internet Corporation for Assigned Names and Numbers. — 2006. URL: http://www.ntia.doc.gov/ntiahome/domainname/icann.htm

101. IANA Naming Function Contract. 30 September 2016. URL: https://www.icann.org/iana_pti_docs/151-iana-naming-function-contract-v-30sep16

2. Библиография

Монографии, сборники научных трудов

На русском языке

102. Балуев Д.Г. Информационная революция и современные международные отношения. — Н.Новгород: ННГУ, 2001. 107 с.

103. Бачило И. Л. Информационное право: учебник для вузов. М.: Высшее образование: Юрайт-Издат, 2009. 454 с.

104. Белл Д. Грядущее постиндустриальное общество: опыт социального прогнозирования: пер. с англ. М.: Academia, 1999. 788 с.

105. Бирюков А.В. Современные международные научно-технологические отношения. М.: РОСНОУ, 2014. 488 с.

106. Богатуров А.Д. Очерки теории и политического анализа международных отношений. / А.Д.Богатуров, Н.А.Косолапов, М.А. Хрусталев. М.: НОФМ, 2002. 309 с.

107. Бурутин А. Новые вызовы и угрозы безопасности России: войны будущего станут информационными. // Актуальные военные аспекты обеспечения международной информационной безопасности. / Под ред. С.В. Короткова. М.: ГШВСРоссии, 2008. 92 с.

108. Валлерстайн И. Анализ мировых систем и ситуация в современном мире: пер. с англ. СПб.: Университетская книга, 2001. 416 с.

109. Вершинин М.С. Политическая коммуникация в информационном обществе СПб.: Изд-во Михайлова В.А., 2001. 253 с.

110. Глобальная безопасность: инновационные методы анализа конфликтов / под ред. А.И. Смирнова. М: Общество «Знание» России, 2011. 272 с.

111. Городов О. А. Информационное право: учебник. М.: Проспект, 2009. 248 с.

112. Иноземцев В.Л. Современное постиндустриальное общество: природа, противоречия, перспективы. М.: Логос, 2000. 304 с.

113. Информационное право: актуальные проблемы теории и практики / под ред. И.Л. Бачило. М.: Юрайт, 2008. 530 с.

114. Кастельс М. Информационная эпоха: экономика, общество и культура: пер. с англ. / под научн. ред. О.И. Шкаратана. М.:ГУ-ВШЭ, 2000. 608 с.

115. Кашлев Ю.Б. Информационный взрыв: международный аспект. М.: Международные отношения, 1988. 208 с.

116. Кокошин А.А. Ядерные конфликты в XXI веке (типы, формы, возможные участники). М.: «Медиа-Пресс», 2003. 144 с.

117. Конышев В. Н. Американский неореализм о природе войны: эволюция политической теории. Спб: Наука, 2004. 372 с. URL: http://polit.msu.ru/pub/unn_mpmo/library/%D0%9A%D0%BE%D0%BD%D1%8B%D1%88%D0%B5%D0%B2.pdf

118. Космос: оружие, дипломатия, безопасность / Под ред. А. Арбатова, В. Дворкина; Моск. Центр Карнеги. М.: РОССПЭН, 2009. 175 с.URL: http://carnegieendowment.org/files/12659outer_space_arbatov.pdf

119. Критически важные объекты и кибертерроризм. Ч. 1. Системный подход к организации противодействия / О.О. Андреев и др.; под ред. В.А. Васенина. М.: МЦНМО, 2008. 398 с.

120. Критически важные объекты и кибертерроризм. Ч. 1. Системный подход к организации противодействия / О.О. Андреев и др.; под ред. В.А. Васенина. М.: МЦНМО, 2008. 398 с.

121. Кузьмин Е.И. Всемирный саммит по вопросам информационного общества / Е.И. Кузьмин, В.Р. Фирсов. СПб: Изд-во РНБ, 2004 135 с.

122. Курбалиа Й. Управление Интернетом / пер. с англ. М.: Координационный центр национального домена сети Интернет, 2010. 208 с.

123. Лебедева М.М. Мировая политика. М.: Аспект-пресс, 2013. 256 с.

124. Международные отношения России в «новых политических пространствах»: космос, приполярные зоны, воздушные и морские пространства, глобальная информационная сфера. М.: URSS, 2011. 272 с.

125. Мировое комплексное регионоведение / Под ред. А.Д. Воскресенского. М.: Магистр-Инфра-М, 2014. 416 с.

126. Наумов В.Б. Право и Интернет: очерки теории и практики. — М.: Книжный дом «Университет», 2002. 432 с.

127. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт. М.: Норма, 2004. 220 с.

128. Политические коммуникации: учебное пособие / под.ред. А.И. Соловьева. М.: Аспект Пресс, 2004. 332 с.

129. Почепцов Г.Г. Информационно-психологическая война. М.: СИНТЕГ, 2000. 179 с.

130. Роговский Е.А. Кибер-Вашингтон: глобальные амбиции. М.: Международные отношения, 2014. 846 С.

131. Роговский Е.А. США информационное общество: экономика и политика. М.: Международные отношения, 2008 408 с.

132. Россия и международная безопасность в космосе / Под ред. А.А. Кокошина. М.: URSS, 2013. 272 с.

133. Серго А. Г. Интернет и право. М.: Бестселлер, 2003 272 с.

134. Современное состояние и перспективы развития военного сотрудничества Российской Федерации в области международной информационной безопасности / Под общ.ред. С.А. Комова. М.: Министерство обороны, 2014.

135. Теория и практика информационного противодействия экстремистской и террористической деятельности: монография. / Судиев И.Ю., Смирова А.А., Кундетов А.И., Федотов В.П. МВД РФ Москва-Вологда: Полиграф-Книга, 2014.

136. Технологический прогресс и современные международные отношения / под общ. ред. А.В. Крутских. М.: Просвещение, 2004. 446 с.

137. Урсул, А. Д. Природа информации: философский очерк Челяб. гос. акад. культуры и искусств; Науч.-образоват. центр «Информационное общество»; Рос. гос. торгово-эконом. ун-т; Центр исслед. глоб. процессов и устойчивого развития. 2-е изд. Челябинск, 2010. 231 с.

138. Уэбстер Ф. Теории информационного общества: пер. с англ. — М.: Аспект-Пресс, 2004. 400 с.

139. Федоров А.В. Информационная безопасность в мировом политическом процессе. М.: МГИМО (У), 2006 218 с.

140. Хрусталев М.А. Анализ международных ситуаций и политическая экспертиза: очерки теории и методологии М.:НОФМО, 2008 232 с.

141. Хрусталев М.А. Системное моделирование международных отношений. М.: МГИМО, 1987. 115 с.

142. Шваб К. Четвертая промышленная революция. М.: ЭКСМО, 2017. 208 с.

143. Экономика и политика в современных международных конфликтах / Под ред. А.Д. Богатурова. М.: Издательство ЛКИ, 2008 336 с.

144. Ядерное сдерживание и нераспространение /Под ред. А.Г. Арбатова и В. Г. Дворкина. М.: Московский Центр Карнеги, 2005. URL: http://carnegieendowment.org/files/9268Nuclear_Deterrence_and_Non-Proliferation.pdf

На иностранных языках

145. Archer C. International organizations. London: Routledge, 2001. 204 p.

146. Arquilla J., Ronfeldt D. Networks and netwars: The future of terror, crime, and militancy. Rand Corporation, 2001.380 p. URL: https://www.rand.org/pubs/monograph_reports/MR1382.html

147. Axelrod R. The Evolution of Cooperation. N. Y.: Cambridge University Press, 1984. 224 p.

148. Banerjee I. The Internet and Governance in Asia: a Critical Reader. Singapore: AMIC, 2007. 380 p.

149. Barkin J.S. Internetional Organizations: Theories and Institutions. N.Y.: Palgrave Macmillan, 2006 185 p.

150. Benedek W. Internet Governance and the Information Society: Global Perspectives and European Dimensions. / W.Benedek, V.Bauer, M.Kettemann. Utrecht: Eleven International Publishing, 2008. 176 p.

151. Buzan B., Wæver O., De Wilde J. Security: a new framework for analysis. Lynne Rienner Publishers, 1998. 239 p.

152. Castells M. End of Millennium. Volume 3, The Information Age: Economy, Society and Culture. Oxford: Blackwell Publishers, 1998. 418 p.

153. Castells M. The Rise of the Network Society: The Information Age: Economy, Society, and Culture. John Wiley & Sons, 2011. 594 p.

154. Cavelty M. The Resurgence of the State: Ttrends and Processes in Cyberspace Governance / M.Cavelty, M.Dunn, S.Krishna-Hensel, V.Mauer. Asghate: Ashgate Publishing, Ltd., 2007. 165 p.

155. Chadwick A., Howard P. Routledge Handbook of Internet Politics. London: Taylor & Francis, 2008. 496 p.

156. Choucri N. Cyberpolitics in International Relations. MIT Press, 2012. 320 p.

157. Chun W., Keenan T. New Media, Old Media: a History and Theory Reader. London: Routledge, 2006. 418 p.

158. Cooper A. Global Governance and Diplomacy: Worlds Apart? / Cooper A., Hocking B., Maley W. N.Y.: Palgrave Macmillan, 2008. 330 p.

159. Cyberprotest: new media, citizens and social movements / Ed. By W. van d Donk, B. Loader, P. Nixon, D. Rucht. Routlege, 2004. 336 p.

160. Cyber warfare and cyber terrorism. / Ed. by L. Janczewski, A. Colarick. NY: IGI Global, 2007. 565 p. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.670.9033&rep=rep1&type=pdf

161. Cybercrime and Cyberterrorism: Current Issues. / Ed. by Blane J. NY: Novinka Books, 2003. 52 p.

162. Cyberspaces and Global Affairs / ed by S. Costigan, J. Perry. London: Routlege, 2012. 408 p.

163. Dai X. International Istitutions and National Policies. N.Y.: Cambridge University Press, 2007. 200 p.

164. Does Technology Drive History? The Dilemma of Technological Determinism / Ed by L. Marx. MIT Press, 1994. 298 p.

165. Franda M. Governing the Internet: The Emergence of an International Regime. Boulder: Lynne Rienner Publishers, 2001. 255 p.

166. Franda M. Launching into Cyberspace. Boulder: Lynne Rienner Publishers, 2002. 297 p.

167. Friedman T. The Lexus and the Olive Tree. N.Y.: Farrar Straus & Giroux,, 1999 394 p.

168. Friedman T. The World is Flat: a Brief History of the Twenty-first Century. N.Y.: Farrar, Straus and Giroux, 2007. 660 p.

169. Security in Cyberspace: Targeting Nations, Infrastructures, Individuals. / Ed by G. Giacomello. Bloomsbury Publishing USA, 2014.256 p.

170. Gerring J. Case study research: principles and practices. Cambridge University Press, 2006. 271 p.

171. Global Governance. Critical Perspectives / ed. by R.Wilkinson, S.Hughes London: Routledge, 2003. 240 p.

172. Goldsmith J., Wu T. Who Controls the Internet? Oxford: Oxford University Press, 2006. 226 p.

173. Goldstein J. International Relations. Washington, D.C.: Longman, 2004. 594 p.

174. Governance.com: Democracy in the Information Age / ed. by C.Kamarck, J. Nye. Washington, D.C.: Brookings Institution Press, 2002. 192 p.

175. Graz J., Nölke A. Transnational Private Governance and its Limits. London: Routledge, 2007. 274 p.

176. Hasenclever A., Mayer P., Rittberger V. Theories of International Regimes. N.Y.: Cambridge University Press, 1997. 248 p.

177. International Cooperation: the Extents and Limits of Multilateralism / ed. by W. Zartman, S. Touval. Cambridge: Cambridge University Press, 2010. 290 p.

178. International critical information infrastructure protection handbook 2008 / 2009 / ed. by A. Wenger, V. Mauer, M. Cavelty. ETH Zurich: Center for Security Studies, 2009. 652 p.

179. International Relations and Security in the Digital Age / Ed. by J. Eriksson, G.Giacomello. Routlege, 2007. 256 p.

180. Internet Governance Forum (IGF): The First Two Years / ed. by A.Doria, W.Kleinwächter. 2008. URL: http://www.intgovforum.org/cms/index.php/component/content/article/57-2008igf/311-internet-governance-forum-the-first-two-years

181. Internet Governance: A Grand Collaboration / ed. by D. MacLean. N.Y.: UN ICT Task Force Series, 2005. 393 p.

182. Kalathil S., Boas T. C. Open networks, closed regimes: The impact of the Internet on authoritarian rule. – Carnegie Endowment, 2010.

183. Keohane R. International Institutions and State Power: Essays in International Relations Theory. Boulder: Westview Press, 1989. 270 p.

184. Keohane R. O. After hegemony: Cooperation and discord in the world political economy. Princeton University Press, 2005. 312 p.

185. Kindleberger Ch. The world in depression, 1929-1939. Berkeley: University of California Press, 1973. 300 p.

186. Krasner S. International Regimes. Ithaca: Cornell University Press, 1983. 372 p.

187. Lessig L. Code and Other Laws of Cyberspace. N. Y.: Basic Books, 1999. 297 p.

188. Lessig L. The Future of Ideas. (The Fate of the Commons in a Connected World). N. Y.: Random House, 2001. 352 p.

189. Libicki M. Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND Corporation, 2009. 240 p.

190. Malcolm J. Multi-Stakeholder Public Policy Governance and its Application to the Internet Governance Forum: thesis for the degree of Doctor of Philosophy – Murdoch University, 2008. 530 p.

191. Mathiason J. Internet Governance: The New Frontier of Global Institutions. London: Taylor & Francis, 2008. 178 p.

192. Mathiason J. Invisible Governance: International Secretariats in Global Politics. Kumarian Press, 2007. 295 p.

193. Mearsheimer J. The tragedy of great power politics. WW Norton & Company, 2001. 592 p.

194. Mcluhan M. Understanding media. The extensions of man. London and NY: McGraw-Hill, 1964. 396 p.

195. Miller, S. Civilizing Cyberspace: Policy, Power, and the Information Superhighway.N.Y.: ACM Press, 1996. 413 p.

196. Molander R. Strategic Information Warfare: A New Face of War / R. Molander, A. Riddile, P. Wilson. CA: Rand Corporation, 1996. 113 p.

197. Morgenthau H. Politics among nations: the struggle for peace and power. 5th edition. NY : Alfred A. Knopf, 1973. 617 p.

198. Mueller M. Ruling the Root: Internet Governance and the Taming of Cyberspace. London: MIT Press, 2002. 327 p.

199. Nye J. The Future of Power in the 21st Century, N.Y.: Public Affairs Press, 2011. 300 p.

200. Price M. E. Media and sovereignty: The global information revolution and its challenge to state power. MIT Press, 2004. 326 p.

201. Poster M. The second media age. NY: Willey Blackwell, 1995. 200 p.

202. Rauscher K., Korotkov A.Working towards rules for governing cyber conflict.Rendering Geneva and Hague conventions in cyberspace // East-West institute. 2011. URL:http://www.ewi.info/working-towards-rules-governing-cyber-conflict

203. Regional cooperation. Regional International Institutions in Comparative Perspective. / Ed by Acharya F., Johnston A. N.Y.: Cambridge University Press, 2007. 318 p.

204. Reinalda B., Verbeek B. Autonomous Policy Making by International Organizations. London: Routlege, 1998. 235 p.

205. Rheingold H. The virtual community: Homesteading on the electronic frontier. – MIT press, 1993. 480 p.

206. Rosenau J. Turbulence in World Politics: A Theory of Change and Continuity. Princeton: Princeton University Press, 1990. 480 p.

207. Rosenau J., Czempiel E. Governance Without Government: Order and Change in World Politics. Cambrige: Cambridge University Press, 1992. 311 p.

208. Ruggie J. Constructing the World Polity: Essays on International Institutionalization. Lonon: Routledge, 1998. 312 p.

209. Schwabach A. Internet and the Law: Technology, Society, and Compromises. Santa Barbara: ABC-CLIO, 2005. 395 p.

210. Securing Outer Space: International Relations Theory and the Politics of Space. / Ed by N. Bormann, M. Sheehan. London: Routledge, 2009. 272 p.

211. Shapiro A. The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World we Know. N.Y.: Public Affairs, 1999. 286 p.

212. Siochru S. Global Media Governance: A Beginner s Guide. / Siochru S., Girard B., Mahan A. Lanham: Rowman & Littlefield, 2002. 202 p.

213. Skolnikoff E. B. The elusive transformation: science, technology, and the evolution of international politics. Princeton University Press, 1994. 336 p.

214. Tallinn Manual on the International Law Applicable to Cyber Warfare. / Ed. by M.Schmitt N.Y.: Cambridge University Press, 2013. 282 p.

215. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. / Ed. by M.Schmitt N.Y.: Cambridge University Press, 2017. 638 p.

216. The Oxford Handbook of Political Science / Ed by R. Goodin. Oxford University Press, 2009. 1320 p.

217. The Politics of Global Governance: International Organizations in an Interdependent World. / Ed. by P. Diehl London: Lynne Rienner Publishers, 2001. 515 p.

218. The political economies of media: The transformation of the global media industries. / Ed by Winseck D. Bloomsbury Publishing, 2011. 321 p.

219. The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment / Ed. By Kleinwächter W. Berlin: Wagner Translations Ltd., 2007. 294 p.

220. Toffler A. Powershift: Knowledge, Wealth, and Violence in the 21st Century. N.Y.: Bantam Books, 1990. 585 p. URL:http://www.rand.org/pubs/monographs/MG877

221. Waltz K. N. Theory of international politics. – Waveland Press, 2010.

222. Young O. Creating Regimes: Arctic Accords and International Governance. Ithaca: Cornell University Press, 1998. 230 p.

223. Young O. Governance in World Affairs. Ithaca: Cornell University Press, 1999. 224 p.

224. Young O. International Cooperation: Building Regimes for Natural Resources and the Environment. Ithaca: Cornell University Press, 1989. 248 p.

225. Young O. International Governance – Protecting Environment in a Stateless Society. Ithaca: Cornell University Press, 1994. 221 p.

226. Zacher M., Sutton B. Governing Global Networks: International Regimes for Transportation and Communication. NY: Cambridge University Press, 1996. 299 p.

227. Zittrain J. The Future of the Internet and How to Stop it. New Heaven, London: Yale University Press, 2008. 352 p.

Статьи и главы в научных и периодических изданиях, научные доклады, диссертации

На русском языке

228. Аничкина Т.Б. О некоторых приемах информационной войны США // США-Канада: экономика, политика, культура. 2007. № 7. С. 123-127.

229. Афонцев С.А. Экономическая политика в современном мире: «глобальное управление» или глобальный политический рынок? // Мировая политика и международные отношения на пороге нового тысячелетия / отв. ред. и авт. введ. М.М. Лебедева МОНФ. Научные доклады № 104. М.: МОНФ, 2000. С. 29-61.

230. Багиров А.Т. Интернет как фактор в глобализации международных отношений: Дисс... канд. полит. наук: 23.00.04 / МГИМО(У) МИД России. М., 2002. 198 с.

231. Багиров А.Т. Новые информационные технологии в международных отношениях // Международная жизнь. 2001. № 8. С. 90-96.

232. Балуев Д.Г. Гражданское общество и глобальное гражданское общество как новые участники многоуровнего международного сотрудничества // НАТО и Россия в глобальном гражданском обществе. М., 2005. С. 75-107.

233. Барабанов О.Н. Глобальное управление и глобальное сотрудничество // Глобализация: человеческое измерение / отв. ред и авт. введ. М.М. Лебедева - М.: РОССПЭН, 2002. С.31-53.

234. Барановский В.Г. Международные организации как механизмы регулирования международных отношений / В.Г.Барановский, Д.В. Алгульян, Е.П. Бажанов // Современные международные отношения / под ред. А.В. Торкунова. М.: РОССПЭН, 1999. С. 220-259.

235. Батуева Е.В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая // Дисс. … ученой степени кандидата политических наук. М.: МГИМО, 2015.

236. Бедрицкий А.В. Международные договорённости по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. 2012. №4. URL: http://www.riss.ru/images/pdf/journal/2012/4/10_.pdf

237. Бедрицкий А.В. «Информационное доминирование» США и асимметричное информационное противоборство // США – Канада: экономика, политика, культура. 2007. № 2.

238. Белонучкин Г., Михайловская Е. Политический сегмент российского Интернета, его развитие и перспективы // Интернет и российское общество / под ред. Семенова И. М.: Гендальф, 2002. С. 70-90.

239. Болгов Р.В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях (политические аспекты). Автореф. дис... канд. полит.наук. СПб.: СПбГУ, 2010.

240. Быков А.И. Управление Интернетом как одна из проблем современных международных отношений // Политэкс URL: http://www.politex.info/content/view/438/30/

241. Волынкина Е. Управление Интернетом – время большой политики // ИКС. 2007. № 12. URL: http://www.iks-media.ru/articles/315146.html

242. Воскресенский А.Д. Мировое комплексное регионоведение и перспективы построения незападной (китаизированной) теории международных отношений // Полис. Политические исследования. 2013. № 6. С. 82-96

243. Гилев А.О. Многомерная война и новая оборонная стратегия // Россия в глобальной политике. №5. 2014. URL: http://www.globalaffairs.ru/number/Mnogomernaya-voina-i-novaya-oboronnaya-strategiya-17101

244. Голицына А. За независимый рунет // Ведомости. 24.02.2009. № 32 (2302). URL: http://www.vedomosti.ru/newspaper/article.shtml?2009/02/24/183081

245. Голицына А. Цветкова М. Стратегический Интернет // Ведомости. 09.04.2009. №63 (2333). URL: http://www.vedomosti.ru/newspaper/article.shtml?2009/04/09/190287

246. Градов А. Деятельность североатлантического союза в сфере кибербезопасности (2014) // Зарубежное военное обозрение. 2014, №7, С. 13-16. URL: http://factmil.com/publ/strana/nato/dejatelnost_severoatlanticheskogo_sojuza_v_sfere_kiberbezopasnosti_2014/61-1-0-452

247. Гуржий А. О программе ЮНЕСКО «Информация для всех» и участии в ней Российской Федерации: (справка) // Программа ЮНЕСКО «Информация для всех»: официальный сайт. URL: http://www.ifap.ru/404.htm

248. Демидов О.В. Обеспечение международной информационной безопасности и российские национальные интересы // Индекс Безопасности. 2013. № 1. С. 136. URL: http://www.pircenter.org/media/content/files/10/13559089230.pdf

249. Демидов О.В. Шесть коротких замечаний относительно Таллиннского руководства CCDCOE // ПИР-Центр: официальный сайт. URL:http://pircenter.org/media/content/files/11/13724548110.pdf

250. Демидов О. Социальные сетевые сервисы в контексте международной и национальной безопасности //Индекс безопасности. 2013. №. 1. С. 100-122

251. Евдокимов Е. Политика Китая в глобальном иформационном пространстве // Международные процессы. 2011. № 1(25). URL:http://www.intertrends.ru/twenty-fifth/009.htm

252. Калиновский О.Н. Информационная война – это война? // Военная мысль, 2001, №1. С. 57-58

253. Карасев П.А. Политика безопасности США в глобальном информационном пространстве. Автореферат дис. на соискание …. к.полит.н. по специальности 23.00.04. М.: ИМЭМО РАН, 2015. URL: https://www.imemo.ru/files/File/ru/dis/2015_004_Karasiov_AUTR.pdf

254. Кибербезопасность гражданских ядерных объектов: оценка угрозы и пути ее преодоления. Доклад ПИР-центра. // Индекс безопасности. 2016. № 3-4. Сс. 63-79.

255. Клочихин Е.А. Место межправительственных организаций среди акторов мировой политики // «Приватизация мировой политики»: локальные действия – глобальные результаты / под ред. М.М. Лебедевой. М., 2008. С. 99-115.

256. Ковалева И.В., Жарикова Е.В. Важные инициативы международного союза электросвязи // Электросвязь. 2008. № 11. С. 2-4.

257. Кожевников А.В. О коллективных мерах государств - членов ОДКБ в сфере обеспечения информационной безопасности // Международный терроризм в информационную эпоху: реалии кибертерроризма и кибероружия, терроризм и средства массовой информации: сб. материалов международной конференции. М., 2010. URL:http://catu.su/index.php?option=com_content&view=article&id=155%3A2011-11-18-13-13-16&catid=38%3Aslideshow&Itemid=91

258. Колин К. К. Философия информации и фундаментальные проблемы современной информатики //Almamater (Вестник высшей школы). 2010. №. 1. С. 29-35.

259. Кононов А.А., Черешкин Д.С. Ключевые проблемы обеспечения безопасности национальной информационной инфраструктуры // Информационное общество. 2002. № 1. С 8-18

260. Коротков А.В. Безопасность критических информационных инфраструктур в международном гуманитарном праве / А.В. Коротков, Е.С. Зиновьева // Вестник МГИМО-Университета. 2011. № 4. С. 154-162

261. Крутских А.В. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. 2007. № 1(5). С.28-37. URL:http://www.intertrends.ru/thirteen/003.htm

262. Крутских А.В. Научно-технологическое направление российской дипломатии // Международная жизнь. 2002. № 12. С. 89-102.

263. Крутских А.В., Федоров А.В. О международной информационной безопасности // Международная жизнь. 2000. №2. С. 37-48.

264. Кувалдин В.Б. Глобализация и судьба нации - государства // Космополис. 1999. С.118-122.

265. Кувалдин В.Б. Противоречивый феномен (взгляд на глобализацию) // Современная Европа. 2002. N 4(12). С.28-38.

266. Кукиер К., Майер-Шёнбергер В. Большие данные // Россия в глобальной политике. 2013. № 3. URL: http://www.globalaffairs.ru/number/Bolshie-dannye--16038

267. Куликова А. Возможна ли гонка кибервооружений между Россией и США? // ПИР Центр 28.01.2015. URL: http://pircenter.org/media/content/files/13/14243529940.pdf

268. Лебедева М.М. Новые технологии как политикообразующий фактор в меняющейся структуре современного мира // Мир и Россия на пороге XXI века: Вторые Горчаковские чтения. МГИМО МИД России (23-24 мая 2000 г.) / под.ред. А.В. Торкунова. М.: РОССПЭН, 2001. С. 94-105.

269. Лебедева М.М. Политическая система мира и новые участники международных отношений // Современные международные отношения и мировая политика / отв. ред. А.В. Торкунов М.: Просвещение, 2004. С. 247-269.

270. Лебедева М.М. Современные технологии и политическое развитие мира // Международная жизнь. 2001. №2. С. 45-53.

271. Лебедева Т.П. Каким быть глобальному управлению? // Вестник Московского университета. 2006 г. №1 (21). Управление (государство и общество). URL:http://www.spa.msu.ru/images/File/Vestnik/Lebedeva.pdf

272. Макарьян Д.В. Интернет как инструмент международной политики // Вестник МГУ. Социология и политология. 2007. № 1 С. 171- 174.

273. Манойло А.В. Объекты и субъекты информационного противоборства // Пси фактор, 2003. URL: http://psyfactor.org/lib/psywar24.htm

274. Мельвиль А.Ю. Пространство и время в мировой политике // Космополис. 2007. №2 (18). С. 117-122.

275. Мельвиль А.Ю. Становление транснациональной политической среды и "волны" демократизации // Современные международные отношения и мировая политика: Учебник для вузов / Отв. ред. А.В. Торкунов; МГИМО(У) МИД России. М.: Просвещение, 2004. С. 106-142.

276. Михеев А.Н. Информационно-коммуникационные технологии: глобальные проблемы и/или глобальные возможности? // Современные глобальные проблемы мировой политики / под ред. М.М. Лебедевой. М.: Аспект Пресс, 2008. С.139-152

277. Михеев А.Н. Неправительственные объединения как акторы мировой политики // «Приватизация» мировой политики: локальные действия – глобальные результаты / под ред. М.М. Лебедевой. М.: Аспект Пресс, 2008 С. 116-140.

278. Михеев А.Н. Принятие внешнеполитических решений в условиях развития новых информационных технологий: роль международных неправительственных организаций: Дисс... канд. полит. наук: 23.00.04 / МГИМО(У) МИД России. М., 2005. 195 с.

279. Мозолина О.В. США и международное сообщество: борьба за управление Интернетом // США и Канада: экономика, политика, культура. – 2006. № 4. С. 111-119.

280. Молчанов С.Н. О международной аккредитации общественных организаций: (информационно-аналитический обзор) // Международное агентство культурно-правовой информации. – 2007. URL: http://www.culturallaw.ru/accreditation.pdf

281. Никитенкова М.А. Развитие информационной инфраструктуры в США как приоритет государственного регулирования // США-Канада: экономика, политика, культура. – 2008. № 12. С. 99-112

282. Носетти Д. Кремль «ВКонтакте»: власть и Интернет в России: доклад. // Центр Россия/ННГ, 2011 г. URL:http://www.pircenter.org/kosdata/page_doc/p2734_1.pdf

283. Мировое комплексное регионоведение / Под ред. А.Д. Воскресенского. М.: Магистр-Инфра-М, 2014

284. О развитии электронного правительства в Российской Федерации и готовности федеральных органов исполнительной власти к переходу на оказание государственных услуг населению с использованием Интернета: доклад Института современного развития. – 2009. URL:http://www.slideshare.net/iponomarev/090428-1367992

285. Песков Д.Н. Интернет в мировой политике // Современные международные отношения и мировая политика / под ред. А.В. Торкунова. – М.: Просвещение, 2004. С. 222-247.

286. Песков Д.Н. Интернет в российской политике: утопия и реальность // Полис. 2002. № 1. С. 31-45.

287. Песков Д.Н. Интернет в России: политическая утопия? URL:http://www.nethistory.ru/biblio/1040595057.html

288. Развитие Интернета в регионах России // Информационный бюллетень Яндекс. Осень-зима, 2012. 13 с.

289. Роговский Е.А. Лидерство США в глобальных технология и международная безопасность // США – Канада: экономика, политика, культура. 2007. №9 С.53-70.

290. Роговский Е.А., Шариков П.А. Контроль над Интернетом и международная стабильность // США – Канада: экономика, политика, культура. 2007. № 3. С. 93-111.

291. Роговский Е.А. Выборы в США: успех технологических инноваций // Международная жизнь. 2017. №3. С. 107-122.

292. Росс А., Скотт Б. Социальные СМИ: причина, следствие и реагирование // Вестник НАТО. URL:http://www.nato.int/docu/review/2011/Social_Medias/21st-century-statecraft/RU/index.htm

293. Росс А., Скотт Б. Социальные СМИ: причина, следствие и реагирование // Вестник НАТО. URL:http://www.nato.int/docu/review/2011/Social_Medias/21st-century-statecraft/RU/index.htm

294. Россия онлайн. Влияние Интернета на российскую экономику: отчет / Б.Банке, В. Бутенко, О. Коцур // The Boston Consulting Group. Май, 2011.

295. Сафранчук И.А. Режим нераспространения ядерного оружия // Современные глобальные проблемы мировой политики. / Под ред. М.М. Лебедевой. М.: Аспект-Пресс, 2009. Сс. 127 – 139

296. Сафранчук И.А. Сохранится ли запрет на ядерные испытания // Россия в глобальной политике. 2006. № 3. URL: http://globalaffairs.ru/number/n_6812

297. Белоус В.С., Сафранчук И.А. Безопасность и надежность ядерных аресеналов без испытаний. Доклад российского представительства Центра оборонной информации. М.: Воениздат, 2006.

298. Северс А.В. Стратегия микротаргетирования и роль социальных сетей в политических коммуникациях // Вестник Московского университета. Серия 10. Журналистика, № 2, 2013. С. 38-47

299. Серго А.Г. Как защищаются права в Интернет // Сборник докладов: выставка-семинар "Электронная коммерция-2000". URL:http://www.internet-law.ru/articles/tezisy-vvc.htm.

300. Туронок С.Г. Информационно-коммуникативная революция и новый спектр военно-политических конфликтов // Политические исследования. – 2003. № 1. С. 24-38.

301. Фененко А.В. Военно-техническая модернизация и «циклы» сближения между США и Россией // Международные процессы. 2011. № 2. URL: http://www.intertrends.ru/twenty-sixth/005.htm

302. Фененко А.В. Международное соперничество за освоение общих пространств // Международные процессы. 2010. № 1. URL: http://www.intertrends.ru/twenty-second/003.htm

303. Цветкова Н. Программы Web 2.0 в публичной дипломатии США // США и Канада: Экономика, политика, культура. 2011. №3. С. 109-122.

304. Цыганков П.А. Постмеждународные отношения: реалии и теории // Место и роль России в трансформирующейся системе международных отношений: материалы семинара / Ин-т мировой экономики и междунар. отношений РАН; Нижегородский гос. ун-т. М., 2002. С. 24-34.

305. Черненко Е.В. Холодная война 2.0? Киберпространство как новая арена противостояния // Россия в глобальной политике. 2013. № 2. URL:http://www.globalaffairs.ru/number/Kholodnaya-voina-20-15874

306. Чернобай А. Роль социальных сетей в мобилизации протестных настроений на Ближнем Востоке и в Северной Африкев в январе-марте 2011 года //

Идеологические аспекты военной безопасности. 2011. № 1. URL:http://mod.mil.by/iavb/2011n1/9.pdf

307. Чугунов А.В. Политика и Интернет: политическая коммуникация в условиях развития современных информационных технологий: автореф. дис... канд. полит.наук: 23.00.01 / СПбГУ. СПб., 2000.

308. Чугунов А.В. Развитие информационного общества: теории, концепции и программы: Учебное пособие. - СПб.: Ф-т филологии и искусств СПбГУ, 2007. 98 с.

309. Ширин С.С. Сообщества разработчиков Интернет-проектов // Вестник МГИМО Университета. 2014. № 6. URL: http://vestnik.mgimo.ru/sites/default/files/pdf/09mir_politika_shirin.pdf

310. Якушев М.В. Информационное общество и правовое регулирование: новые проблемы теории и практики // Информационное общество. 1999. № 1. URL:http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/2be96a4e09339699c32568b1003ab653

На иностранных языках

311. Acton J. M. the Problem with nuclear Mind reading //Survival. 2009. №. 1. P. 119-142

312. Aday S. Blogs and bullets. New media in contentious politics // United States Institute of Peace. August 2010. №5. URL:http://www.newmediacenter.ru/wp-content/uploads/2011/10/adayetal2010.pdf

313. Anheier H., Hagai K. Mapping Global Civil Society // Global Civil Society 2003. / ed. by H.Anheier, M.Glasius, M.Kaldor. Centre for Civil Society and Centre for the Study of Global Governance, London School of Economics and Political Science Oxford: Oxford University Press, 2003. P. 241-258.

314. Arimatsu L. A treaty for governing cyber-weapons: Potential benefits and practical limitations // Cyber Conflict (CYCON). 2012. 4th International Conference on. IEEE, 2012.

315. Arts B. Regimes, Non-State Actors and the State System: a ‘Structurational’ Regime Model // European Journal of International Relations. 2000. No 6(513). URL:http://ejt.sagepub.com/cgi/content/abstract/6/4/513

316. Axelrod R., Keohane R. O. Achieving cooperation under anarchy: Strategies and institutions //World politics. 1985. T. 38. №. 1. P. 226-254.

317. Babst S. NATO's New Public Diplomacy: The Art of Engaging and Influencing // Atlantic Community. 20.02.2009. URL:http://www.atlantic-community.org/index/articles/view/NATO's_New_Public_Diplomacy%3A_The_Art_of_Engaging_and_Influencing

318. Baird Z. Governing the Internet: Engaging Government, Business and Non-profits // Foreign Affairs. 2006. -No 6 (81). P. 14-20

319. Baird Z., Verhulst S. A New Model for Global Internet Governance // Governance in the 21st Century: The Partnership Principle, Alfred Herrhausen Society for International Dialogue. URL: http://swandive.securesites.net/downloadable_assets/ahs_global_internet_gov.pdf

320. Barlow J. A Declaration of the Independence of Cyberspace. 1996. URL: http://homes.eff.org/~barlow/Declaration-Final.html

321. Bauer J. Internet Governance: Theory and First Principles // 33rd Research Conference on Communication, Information and Internet Policy. Alexandria, VA. September 23-25, 2005. URL:http://web.si.umich.edu/tprc/papers/2005/441/Bauer-TPRC-2005-fin.pdf

322. Benhamou B., Sorbier L. Souveraineté et Réseaux Numériques // Politique Étrangère. 2006. No 3. URL:http://www.google.com/url?sa=t&source=web&ct=res&cd=1&url=http%3A%2F%2Fwww.netgouvernance.org%2Fpolitiqueetrangere.pdf&ei=yqEZSqWtPJHGsgaA6Nm-Cg&rct=j&q=Souverainet%C3%A9+et+r%C3%A9seaux+num%C3%A9riques+&usg=AFQjCNGLwwRuGri8ijTGu_oScnl1GZabFQ

323. Bertola V. End User Involvement in Internet Governance: Why and How // ITU Workshop on Internet Governance. Geneva, 2004.

324. Brahm E. International Regimes. Beyond Intractability // Conflict Research Consortium. Boulder, University of Colorado. URL:http://www.beyondintractability.org/essay/international_regimes

325. Breitmier H. International Organizations and the Creation of International Environmental Regimes // Global Governance: Drawing Insights from the Environmental Experience / ed. by O. Young. London: MIT Press, 1997. P. 87-115.

326. Brown T. Ideological Hegemony and Global Governance // Conflict Research Consortium. Boulder, University of Colorado. URL:http://cfs.colorado.edu/jwsr/archive/vol3/v3n2a2.htm

327. Callister P. D. The Internet, Regulation and the Market for Loyalties: An Economic Analysis of Transborder Information Flow //University of Illinois Journal of Law, Technology & Policy. 2002. №. 1. P. 59-107.

328. Cammaerts B., Carpentier N. The Unbearable Lightness of Full Participation in a Global Context: WSIS and Civil Society participation. // Towards a Sustainable Information Society: Deconstructing WSIS / ed. by J.Servaes, N.Carpentier Bristol: Intellect Books, 2005. P.17-49.

329. Carr M. Power Plays in Global Internet Governance //Millennium-Journal of International Studies. 2015. T. 43. №. 2. P. 640-659.

330. Castells M. Communication, Power and Counter-power in the Network Society // International Journal of Communication. 2007. № 1. P. 238-266.

331. Castells M. The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance // The Annals of the American Academy of Political and Social Science. 2008. № 616. URL:http://prtheories.pbworks.com/w/file/fetch/45138545/Castells_2008_The_New_Public_Sphere.pdf

332. Charnovitz S. Nongovernmental Organizations and International Law // The American Journal of International Law. 2006. № 2 (100). P. 348-372. URL:http://links.jstor.org/sici?sici=0002-9300%28200604%29100%3A2%3C348%3ANOAIL%3E2.0.CO%3B2-1

333. Civil Movements: The Impact of Facebook and Twitter // Arab social media report. May 2011. № 2(1). URL: http://www.dsg.ae/portals/0/ASMR2.pdf

334. Cogburn D. Globalization and Governance in Cyberspace: Mapping the Processes of Emergent Regime Formation in Global Information and Communications Policy. URL:http://arxiv.org/ftp/cs/papers/0109/0109052.pdf

335. Comments of the Internet Governance Project on The Continued Transition of the Technical Coordination and Management of the Internet's Domain Name and Addressing System: Midterm Review of the Joint Project Agreement submitted to The National Telecommunications and Information Administration U.S. Department of Commerce February 15, 2008. URL:http://www.internetgovernance.org/pdf/IGP-JPA-08-comments.pdf

336. Coste P. La Gouvernance Internationale de l'Internet // Politique étrangère. 2006. No 3. P. 507-518.

337. Cukier K. Multilateral Control of Internet Infrastructure and its Impact on US Sovereignty // Telecommunications Policy and Research Conference. Alexandria, VA. October 2004. URL:http://www.cukier.com/writings/cukier-netgov-TPRC04.pdf.html

338. Cukier K. The Next Internet Governance Battles // The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment / ed. by W. Kleinwächter. Berlin: Wagner Translations Ltd., 2008. P. 285-296

339. Cukier K. The WSIS Wars: an Analysis of the Politicization of the Internet. // The World Summit on the Information Society: Moving from the Past into the Future. / ed. by D. Stauffacher, W. Kleinwächter. N.Y.: UN, ICT Task Force Series, 2005. URL:http://www.cukier.com/writings/cukier-WSISWARS-30may05.html

340. Curtis T. The International Telecommunication Regimes in the Information Age // Prometheus. 2003. No 4 (21). P. 399-414.

341. Dean D. The Connected World. The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy / D. Dean, S. DiGrande, D. Field, P. Zwillenberg // BCG Perspectives. 27.01.2012.

342. Dean D. The Connected World. The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy / D. Dean, S. DiGrande, D. Field, P.

Zwillenberg // BCG Perspectives. 27.01.2012.URL:https://www.bcgperspectives.com/content/articles/growth_innovation_connected_world_digital_manifesto/

343. Dean D. The internet economy in the G-20: The $4.2 trillion growth opportunity //White paper, Boston Consulting Group, 2012.

344. Dichter Th. W. Globalization and Its Effects on NGOs: Efflorescence or a Blurring of Roles and Relevance? // Nonprofit and Voluntary Sector Quarterly. – 1999. – No 28(38). URL:http://nvs.sagepub.com/cgi/content/abstract/28/suppl_1/38

345. Drake W. Reframing Internet Governance Discourse: Fifteen Baseline Propositions // Memo #2 for the Social Science Research Council's Research Network on IT and Governance. URL:http://www.programs.ssrc.org/itic/publications/Drake2.pdf

346. Drake W. The Rise and Decline of the International Telecommunication Regime // Regulating global information society / ed. by Ch. Masrsden London: Routledge, 2000. P. 124-178.

347. Drezner D. The Global Governance of the Internet: Bringing the State back in // Political Science Quarterly. 2004. № 3 (119). URL: http://www.danieldrezner.com/research/egovernance.pdf

348. Drezner D. W., Farrell H. Introduction: Blogs, politics and power: a special issue of Public Choice //Public Choice. 2008. Т. 134. №. 1-2. P. 1-13.

349. Dutton W., Peltu M. The emerging internet governance mosaic: connecting the pieces: Discussion Paper No 5 // Oxford Internet Institute Forum. Oxford, 2005. URL:http://www.iospress.metapress.com/index/M14U6635863R0718.pdf

350. Dutton W., Peltu M. The New Politics of the Internet. Multistakeholder Policy Making and the Internet Technocracy // Routledge Handbook of Internet Politics / ed. by A.Chadwick, P.Howard London: Routledge, 2008. P. 384-401.

351. Emmanuel J., Caral A. Lessons from ICANN: Is Self-Regulation of the Internet Fundamentally Flawed? // International Journal of Law and Information Technology. 2004. No. 12(1). P. 1-31.

352. Fearon J. D. Bargaining, enforcement, and international cooperation // International Organization. 1998. №. 02. P. 269-305.

353. Finkelstein L. What is Global Governance? // Global Governance. 1995. No. 3(1). P. 367-372.

354. Freedom on the Net. A Global assessment of Internet and Digital Media // Freedom House. 01.04.2009. URL:http://www.state.gov/documents/organization/135959.pdf

355. Freedom on the Net. A Global assessment of Internet and Digital Media // Freedom House. 01.04.2009. URL:http://www.state.gov/documents/organization/135959.pdf

356. Froomkin M. International and National Regulation of the Internet // The Round Table Expert Group on Telecommunications Laws: Conference Papers / ed. by E.Dommering, N. Eijk. Amsterdam, 2005. URL: http://law.tm/docs/International-regulation.pdf

357. Fuchs C. Dallas Smythe Reloaded: Critical Media and Communication Studies Today // The audience of commodity in digital age. / Ed. by L. McGuigan, V. Manzerolle. New York: Peter Lang, 2013. P. 267-288.

358. Giles K., Hagestad W. Divided by a common language: cyber definitions in Chinese, Russian and English //Cyber Conflict (CyCon), 2013 5th International Conference on. IEEE, 2013. P. 1-17.

359. Goldschmidt P. The Urgent Need to Strengthen the Nuclear Non-Proliferation Regime //Policy Outlook. 2006. №. 25. URL: http://carnegieendowment.org/files/PO25.Goldschmidt.FINAL.pdf

360. Grieco J. Understanding the Problem of International Cooperation: The Limits of Neoliberal Institutionalism and the Future of Realist Theory // Neorealism and Neoliberalism: the Contemporary Debate. / ed. by D.Baldwin. N. Y.: Columbia University Press, 1993. P. 301-338.

361. Grieco J. M. Anarchy and the limits of cooperation: a realist critique of the newest liberal institutionalism //International organization. 1988. T. 42. №. 03. P. 485-507.

362. Haas P. Epistemic Communities and the Dynamics of International Environmental Cooperation // Regime Theory and International Relations / ed. by V. Rittberger. Oxford: Oxford University Press, 1995. P. 168-202.

363. Haas, P. Epistemic Communities and International-Policy Coordination. Introduction // International Organization. 1992. No. 46 (1) P. 1-35.

364. Hansen L., Nissenbaum H. Digital disaster, cyber security, and the Copenhagen School //International Studies Quarterly. 2009. №. 4. P. 1155-1175.

365. Hasenclever A., Mayer P., Rittberger V. Integrating Theories of International Regimes // Review of International Studies. 2000. No. 26. P. 3–33

366. Haufler V. Crossing the Boundaries Between Public and Private: International Regimes and Non-State Actors // Regime Theory and International Relations / ed. by V. Rittberge. Oxford: Oxford University Press, 1995. P. 94-111.

367. Henderson J. Global production networks and the analysis of economic development / Henderson J. , Dicken P., Hess M., Coe N., Yeung H. //Review of international political economy. 2002. №. 3. P. 436-464.

368. Hofmann J. Internet Governance: A Regulative Idea in Flux // Social Science Research Centre. Berlin, 2005. URL:http://duplox.wzb.eu/people/jeanette/texte/Internet%20Governance%20english%20version.pdf

369. ICANN and Internet Governance: Getting Back to Basics // Center for Democracy and Technology. URL: http://www.cdt.org/dns/icann/20040713_cdt.pdf

370. Judge A. International Organization Networks // International Organization: A Conceptual Approach / Ed. by A.Groom, P.Taylor. London: Pinter Publishers, 1978.

371. Kein H. ICANN and internet governance: leveraging technical coordination to realize global public policy // Information Society. 2002. № 18 (193–207). URL:http://programs.ssrc.org/itic/publications/civsocandgov/Klein.pdf

372. Kennard W. Vision to Mission. A Blueprint for Architects of the Global Information Infrastructure: Speech Before the World Economic Development Congress. 23 September 1999. URL:http://www.fcc.gov/Speeches/Kennard/spwek932.html

373. Keohane R. International Institutions: Can Interdependence Work? (The Frontiers of Knowledge) // Foreign Policy. 1998. Vol. 110. P. 82-96.

374. Khatib L. and al. Public Diplomacy 2.0: An Exploratory Case Study of the US Digital Outreach Team // Oxford Internet Institute. CDDRL working papers. 2011. №

120. URL: http://uscpublicdiplomacy.org/media/Exploratory_Case_Study_US_Digital_Outreach_Team.pdf

375. Klein H. Understanding WSIS: An Institutional Analysis of the UN World Summit on the Information Society // The Massachusetts Institute of Technology Information Technologies and International Development. 2004. № 3–4 (1). P. 3-13.

376. Kleinwächter W. Global Governance in the Information Age // Center for Internet Research, University of Aarhus. 2001. P. 1–46. URL:http://www.palgrave-journals.com/development/journal/v46/n1/abs/1110416a.html

377. Kleinwächter W. De-Mystification of the Internet Root: Do we need Governmental Oversight? // Reforming Internet Governance. Perspectives from the Working Group on Internet Governance / ed. by W. Drake. – N.Y.: UN, ICT Task Force Series, 2005. URL:http://www.wgig.org/docs/book/Wolfgang_Kleinwa%CC%88chter.html

378. Kleinwächter W. Internet Co-Governance. Towards a Multilayer Multiplayer Mechanism of Consultation, Coordination and Cooperation (M3C3) // E–Learning. 2006. No. 3(3). URL:http://www.wwwords.co.uk/pdf/viewpdf.asp?j=elea&vol=3&issue=3&year=2006&article=18_Kleinwachter_ELEA_3_3_web&id=212.16.10.52

379. Klimburg A. The Internet Yalta: Commentary // Center for New American Security. 5.02.2013. URL:http://www.cnas.org/theinternetyalta

380. Kobrin S. Back to the Future: Neomedievalism and the Post Modern Digital World Economy // Columbia Journal of International Affairs. 1998. № 2 (51) . P. 361-386.

381. Kratochwil F., Ruggie J. International Organization: A State of the Art and an Art of the State // International Organization. 1986. No. 40 (4). P. 753–775.

382. Kummer M. Internet Governance and the Need for an Inclusive Multi-Stakeholder Dialogue: Position Paper // Social & economic factors shaping the future of the internet NSF/OECD Workshop. Washington, 2007

383. Levy M, Young O, Zuern M. The Study of International Regimes // European Journal of International Relations. 1995. № 3(1). P. 267-330.

384. Lewis J. Confidence-building and international agreement in cybersecurity // Disarmament Forum. 2011. №4. P. 51-60. URL: https://citizenlab.ca/cybernorms2012/Lewis2011.pdf

385. Lewis J., Timlin K. Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization, UNIDIR, 2011. URL: http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

386. Lichtenstein J. Digital Diplomacy // New York Times Magazine. 16.07.2010. URL:http://www.nytimes.com/2010/07/18/magazine/18web2-0-t.html?pagewanted=all

387. Lieberthal K., Singer P. Cybersecurity and U.S. - China Relations. // Jonh L. Torton China Institute in Brookings, 2012. 52 p. URL: https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf

388. Litan R. Thoughts on Internet Policy and Global Governance: Draft Position Paper // Tokyo Club Meetings. October 2001. URL:http://www.tcf.or.jp/data/20020124-25_Robert_Litan.pdf

389. MacLean D. Herding Cats: Some Conceptual Tools for Thinking about Internet Governance // Internet Governance: a Grand Collaboration: an Edited Collection of Papers / ed. by D. MacLean. N.Y.: UN ICT Task Force, 2004. P. 73-100.

390. Masanga C. The Internet Governance Forum: Its Development, Function and Future // Internet Governance and the Information Society: Global Perspectives and European Dimensions / ed. by W.Benedek, V.Bauer, M.Kettemann. Utrecht: Eleven International Publishing, 2008. P. 63-79.

391. Mathiason J. Internet Governance: The State of Play: Report Commissioned by the UN ICT Task Force / J.Mathiason, M.Mueller, H.Klein, M.Holitscher, L.McKnight — 2004. URL:http://dcc.syr.edu/miscarticles/MainReport-final.pdf

392. McLaughlin L., Pickard V. What is Bottom-up about Global Internet Governance? — Global Media and Communication. 2005. № 1(3) P. 357–373.

393. Mearsheimer, J. The False Promise of International Institutions // International Security. 1994. No. 15. P. 5–49.

394. Menthe D. Jurisdiction in Cyberspace: A Theory of International Spaces // Michmann Telecommunication Technical Revue. № 69. URL:http://www.law.umich.edu/mttlr/vol-four/menthe.html

395. Morozov E. The Digital Dictatorship // Wall Street Journal. 20.02.2010. URL:http://online.wsj.com/article/SB10001424052748703983004575073911147404540.html

396. Mueller M. Dancing the Quango: ICANN as International Regulatory Regime // Johns Hopkins SAIS / George Mason University Conference on Technology and Global Governance. February 11-12, 2002. URL: http://istweb.syr.edu/~mueller/quango.pdf

397. Mueller M. Making Sense of Internet Governance: Defining Principles and Norms in a Policy Context / M.Mueller, J.Mathiason, L.McKnight // Internet Governance Project, 2004. URL:http://dcc.syr.edu/reports.htm

398. Mueller M. Network Neutrality as Global Principle for Internet Governance / M.Mueller, D. Cogburn, J.Mathiason, J.Hoffmann // Internet Governance Project: Official Site. – 2007. URL:www.internetgovernance.org/pdf/NetNeutralityGlobalPrinciple.pdf

399. Mueller M. Political Oversight of ICANN: A Briefing for the WSIS Summit: Concept Paper by the Internet Governance Project / M.Mueller, K H.lein, J.Hofmann, L.McKnight, D.Cogburn 2005. URL: www.world-governance.org/spip.php?article135

400. Mueller M. The Internet and Global Governance: Principles and Norms for a New Regime / M.Mueller, J.Mathiason, H.Klein // Global Governance. – 2007. – № 13. URL:http://www.atypon-link.com/LRP/doi/abs/10.5555/ggov.2007.13.2.237

401. Neuneck G. Civilian and military cyberthreats: shifting identities an attribution. // The Cyber Index. International Security Trends and Realities. UNIDIR, 2013.P. 115 // http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

402. Nojeim G. Statement On Cybersecurity, Civil Liberties and Innovation. // US Senate House Committee on Energy and Commerce, Subcommittee on

Communications, Technology and the Internet. Washington D.C., 1st may 2009. URL:http://www.cdt.org/security/20090501_cybersecurity.pdf

403. Norton cybercirme report 2013. // Symantec official site. URL: http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.pptx

404. Nye J. Nuclear lessons for cyber security. Air Univ Press Maxwell Afb Al, 2011.

405. Nye J. Cyberpower // Belfer center for science in international affairs. 2010. URL:http://www.dtic.mil/dtic/tr/fulltext/u2/a522626.pdf

406. Nye J., Owens W. America's Information Edge // Foreign Affairs. 1996. March-April. P. 20-36.

407. Panke D. Lock-in Strategies in International Negotiations: The Deconstruction of Bargaining Power //Millennium-Journal of International Studies. 2015. №. 2. P. 375-391.

408. Peterson M. International organizations and the implementation of the environmental regimes // Global Governance: Drawing Insights from the Environmental Experience / ed. by O. Young. London: MIT Press, 1997. P. 115-153.

409. Pickard V. Neoliberal Visions and Revisions in Global Communications Policy From NWICO to WSIS // Journal of Communication Inquiry. 2007. № 2(31). P. 118-139.

410. Price M. E. The market for loyalties: Electronic media and the global competition for allegiances //Yale Law Journal. 1994. P. 667-705.

411. Raboy M. The Origins of Civil Society Involvement in the WSIS // The International Journal of Communication Studies. 2004.№ 3–4 (1). P. 225-232.

412. Raboy M. The World Summit on the Information Society and its Legacy for Global Governance // The international journal for communication studies. 2004. № 3-4 (66). P. 225–232.

413. Rauscher K. F., Yaschenko V. Russia–US Bilateral on Cyber Security: Critical Terminology Foundations //New York, USA: EastWest Institute. 2011.

414. Rauscher K., Korotkov A. Working towards rules for governing cyber conflict. Rendering Geneva and Hague conventions in cyberspace // East-West institute. 2011. URL:http://www.ewi.info/working-towards-rules-governing-cyber-conflict

415. Reardon R., Choucri N. The Role of Cyberspace in International Relations: A View of the Literature. 2012. // Paper Prepared for the 2012 ISA Annual Convention. San Diego, CA.1.04. 2012. URL: http://ecir.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf

416. Reidenberg J. Lex Informatica: The Formulation of Information Policy Rules Through Technology // Texas Law Review. 1998. No 3 (76). P. 553-584.

417. Risen T. China, Russia Seek New Internet World Order // US News and World Report. 14.05.2015. URL: http://www.usnews.com/news/articles/2015/05/14/china-russia-seek-new-internet-world-order

418. Ristow B. The New Gatekeepers: Controlling Information in the Internet Age. A report to the Center for International Media Assistance // Center for International Media Assistance. 2013. URL: http://apo.org.au/files/Resource/CIMA_TheNewGatekeepers_May2013.pdf

419. Ristow B. The New Gatekeepers: Controlling Information in the Internet Age // Center for International Media Assistance. 2013. 25 p.

420. Rogerson K. Information Interdependence: Keohane and Nye's Complex Interdependence in the Information Age // Communication & Society. 2000. № 3 (3). P. 415-436.

421. Rosato S. The Inscrutable Intentions of Great Powers //International Security. 2015. №. 3. P. 48-88.

422. Rosenau J. Governance in the 21st Century // Global Governance: a Review of Multilateralism and International Organization. 1995. № 1 (1). P. 13-43.

423. Rosenau J. States, Sovereignty, and Diplomacy in the Information Age: Paper prepared for Presentation at the Panel on «Virtual Diplomacy: A Revolution in Diplomatic Affairs Theory», Annual Meeting of the International Studies Association. Washington, D.C. February 18, 1998. URL:http://www.usip.org/virtualdiplomacy/publications/reports/jrosenauisa99.html

424. Rothkopf D. Cyberpolitik: the Changing Nature of Power in the Information Age — Journal of International Affairs. 1998. № 2(51). P. 325-359.

425. Ruggie J. International Regimes, Transactions and Change: Embedded Liberalism in the Postwar Economic Order // International Regimes / Ed. by S. Krasner. Ithaca: Cornell University Press, 1983. P. 195-233.

426. Sadowsky J. Intrenet Governance: a Discussion Document: Prepared for the UN ICT Task Force / J.Sadowsky, R.Zambrano, P.Dandjinou. N.Y., 2004. URL:http://www.apdip.net/resources/e-governance/igov/link.2005-07-18.3464395395/view

427. Shaw R. Reflection on Governments, Governance and Sovereignty in the Internet Age. August 24, 1999. URL:http://web.archive.org/web/20010112082400/http://people.itu.int/~shaw/docs/reflections-on-ggs.htm

428. Stayner J. Web 2.0 and the transformation of news and journalism // Handbook of Internet Politics. / Ed by A. Chadwick, London: Routledge, 2008. P. 201-213.

429. Stein A. Coordination and Collaboration: regimes in an Anarchic World // International Organization.1982. № 2 (36). P. 299-324.

430. Stokke O. Regimes as governance systems // Global governance: drawing Insights from the environmental experience / ed. by O. Young NY: Cambridge University Press, 1997. —P. 27-63

431. Survey of Developments in Electronic Money and Internet and Mobile Payments: Banc of International Settlements, Committee on Payment and Settlement Systems, 2004. URL:http://www.bis.org/publ/cpss62.pdf

432. Szafranski R. A Theory of Information Warfare: Preparing for 2020 / Airpower Journal, 1995 №1. URL: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA328193

433. Tannenwald N. Law versus power on the high frontier: The case for a rule-based regime for outer space //Yale Journal on International Law. 2004. URL: http://drum.lib.umd.edu/bitstream/1903/7902/1/tannenwald.pdf

434. Tech@State // US Department of State: official site. URL:http://www.state.gov/statecraft/tech/index.htm

435. Tech@State: Serious Games Conference Unlocks Human Potential Through Play // Dipnote US: Department of State Official Blog. 6.07.2011. URL:http://blogs.state.gov/index.php/site/entry/techstate_serious_games_conference

436. The future of the internet. A virtual counter-revolution // Economist. 2.09.2010. URL:http://www.economist.com/node/16941635

437. The Struggle Over Internet Governance: Searching For Common Ground: Draft Position Papers for Discussion Forum Oxford Internet Institute. University of Oxford. 6th May, 2005. URL: http://www.oii.ox.ac.uk/collaboration/?rq=specialevents/20050505

438. Vetter T. Internet Governance Forum: A development perspective. A primer for the third meeting. Hyderabad, India. 3–6 December, 2008. URL:www.iisd.org/publications/pub.aspx?id=994

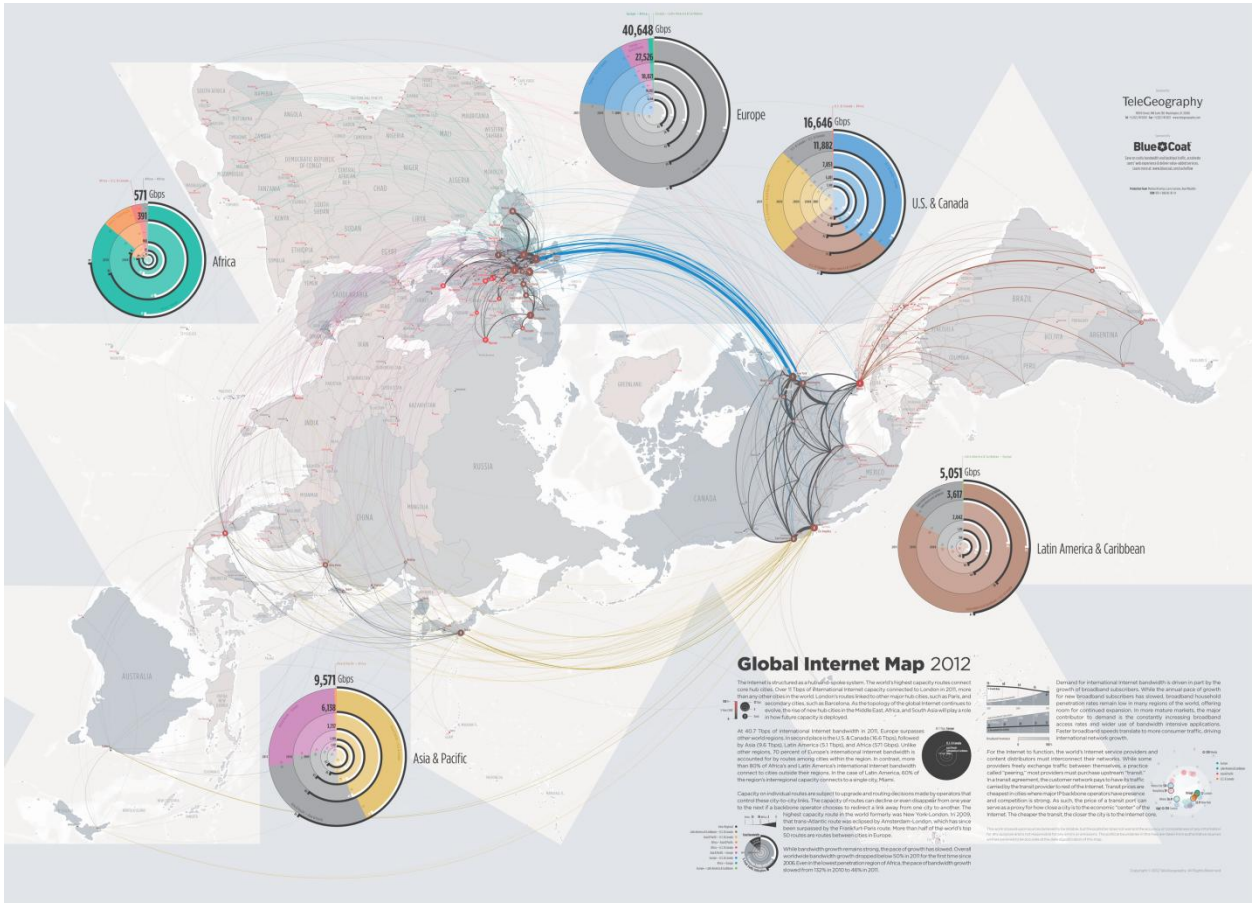
439. Walt S. M. The renaissance of security studies //International Studies Quarterly. 1991. P. 211-239.

440. Warkentin C., Mingst K. International Institutions, the State, and Global Civil Society in the Age of the World Wide Web // Global Governance. 2000. № 6 (2). P. 237-255.

441. Wendt A. Constructing International Politics // International Security. 1995. № 1(20). P. 71-81.

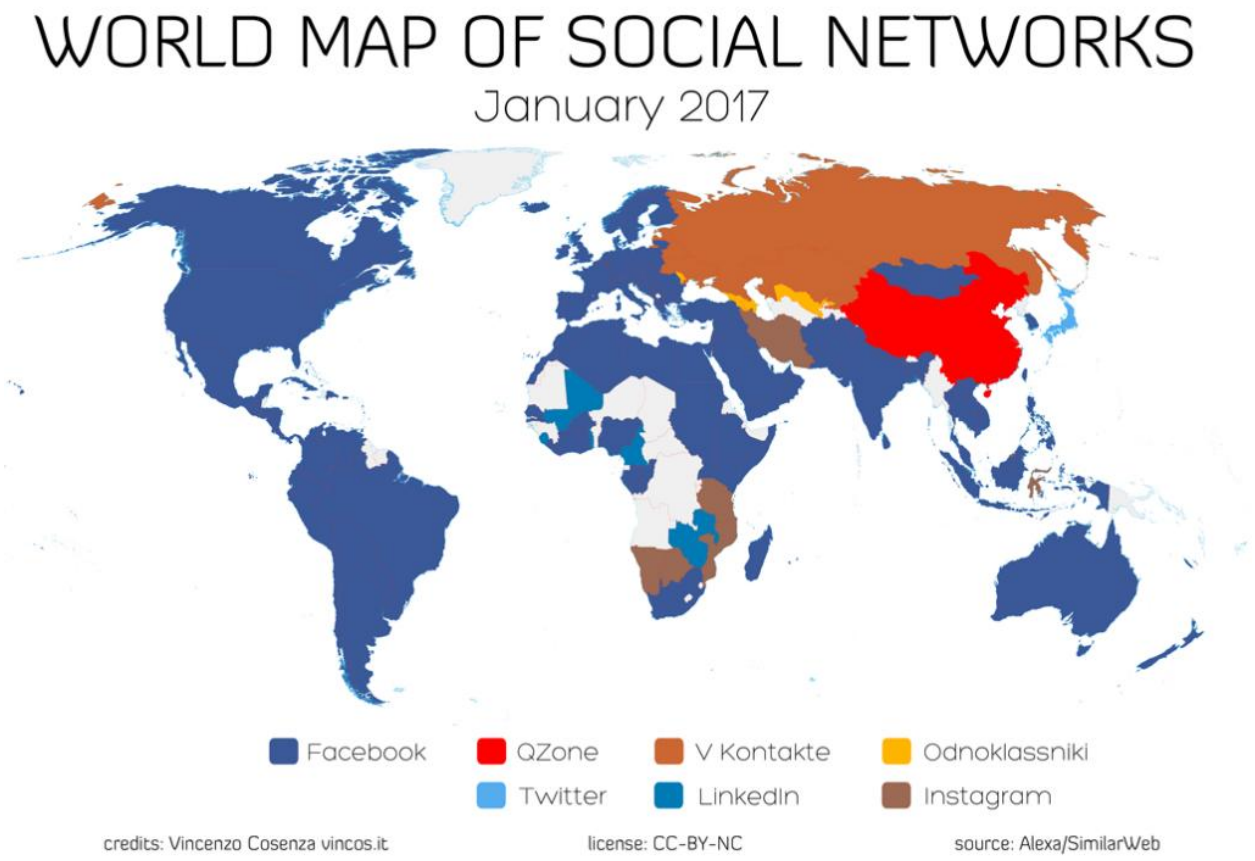
442. Wenger A. The Internet and the Changing Face of International Relations and Security // Information and Security. 2001. № 7. P. 5-11.

Приложение 1.
Потоки пакетноготрафика в глобальном информационном пространстве



Ист: Global Internet Map 2012. Telegeorgaphy. URL: http://telecomblogs.in/wp-content/uploads/2010/04/internet_map_2010_lg1.png

Приложение 2.
Использование социальных сетевых сервисов в странах мира



Ист: World map of social networks. 2017. URL:www.alexa.com

Приложение3.
Понятийный аппарат[538]

«интернет вещей» - концепция вычислительной сети, соединяющей вещи (физические предметы), оснащенные встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой без участия человека;

«информационная безопасность» — состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве;

«информационная война» — противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны;

«информационная инфраструктура» — совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации;

«информационное оружие» — информационные технологии, средства и методы, применяемые в целях ведения информационной войны;

«информационная преступность» — использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях;

---

[538] Источники: Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности // МИД России. Официальный сайт. 8.05.2015. URL: http://www.mid.ru/brp_4.nsf/newsline/2C7A7D0752AAB2B843257E3F003F2204; Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2009 г. // Международная информационная безопасность: дипломатия мира: сборник материалов / под ред. С.А. Комова. М., 2009; Rauscher K. F., Yaschenko V. Russia–US Bilateral on Cyber Security: Critical Terminology Foundations //New York, USA: East West Institute. 2011; Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. Утверждена указом Президента 09.05.2017. № 203. URL: http://kremlin.ru/acts/bank/41919

«информационное пространство» — сфера деятельности, связанная сформированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию;

«информационное общество» - общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан;

«информационные ресурсы» — информационная инфраструктура, а также собственно информация и ее потоки;

«информационный терроризм» — использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях;

«критически важные структуры» — объекты, системы и институты государства, воздействие на которые может иметь последствия, прямо затрагивающие национальную безопасность, включая безопасность личности, общества и государства;

«международная информационная безопасность» — состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве;

«несанкционированное вмешательство в информационные ресурсы» — неправомерное воздействие на процессы формирования, создания, обработки, преобразования, передачи, использования, хранения информации;

«угроза информационной безопасности» — факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве;

«киберпространство» - электронная (включая фотоэлектронные и пр.) среда, в которой информация создается, передается, принимается, хранится и уничтожается;

«киберконфликт» - напряженная ситуация между и / или среди государств политически организованных групп, при которой враждебные (нежелательные) кибератаки приводят к ответным действиям;

«кибервойна» - высшая степень киберконфликта между или среди государств, во время которой государства предпринимают кибератаки против критических информационных инфраструктур противника как часть военной кампании; может быть объявлена формально одной (всеми) конфликтующими сторонами, или может не объявляться формально и быть de facto;

«кибератака» - наступательное использование кибероружия с целью нанесения вреда определенной цели;

«наступательный потенциал в киберпространстве» - возможность начать кибератаку, которая может быть использована в качестве средства сдерживания в киберпространстве;

«кибероружие» - совокупность технических и программных средств, применяемых для нарушения нормальной работы и/ или доступности кибер-инфраструктуры, сервисов, ресурсов;

«облачные вычисления» - информационно-технологическая модель обеспечения повсеместного и удобного доступа с использованием сети "Интернет" к общему набору конфигурируемых вычислительных ресурсов ("облаку"), устройствам хранения данных, приложениям и сервисам, которые могут быть оперативно предоставлены и освобождены от нагрузки с минимальными эксплуатационными затратами или практически без участия провайдера.