ИССЛЕДОВАТЕЛЬСКИЙ ПРОЕКТ
МЕЖДУНАРОДНОГО ИССЛЕДОВАТЕЛЬСКОГО
КОНСОРЦИУМА ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

МЕТОДОЛОГИЧЕСКИЕ ВОПРОСЫ ПРИМЕНЕНИЯ НОРМ, ПРАВИЛ И ПРИНЦИПОВ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ, ПРИЗВАННЫХ СПОСОБСТВОВАТЬ ОБЕСПЕЧЕНИЮ ОТКРЫТОЙ, БЕЗОПАСНОЙ, СТАБИЛЬНОЙ, ДОСТУПНОЙ И МИРНОЙ ИКТ-СРЕДЫ

Под редакцией
Проф. Анатолия Стрельцова
Др. Энекен Тикк

ИССЛЕДОВАТЕЛЬСКИЙ ПРОЕКТ МЕЖДУНАРОДНОГО ИССЛЕДОВАТЕЛЬСКОГО КОНСОРЦИУМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДОЛОГИЧЕСКИЕ ВОПРОСЫ ПРИМЕНЕНИЯ НОРМ, ПРАВИЛ И ПРИНЦИПОВ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ, ПРИЗВАННЫХ СПОСОБСТВОВАТЬ ОБЕСПЕЧЕНИЮ ОТКРЫТОЙ, БЕЗОПАСНОЙ, СТАБИЛЬНОЙ, ДОСТУПНОЙ И МИРНОЙ ИКТ-СРЕДЫ

Под редакцией
Проф. Анатолия Стрельцова
Др. Энекен Тикк

2020

УДК 004.056
ББК 32.97
М54

УЧАСТНИКИ ПРОЕКТА

Анатолий Стрельцов, Московский государственный университет, Национальная ассоциация международной информационной безопасности, Российская Федерация

Валерий Ященко, Московский государственный университет, Российская Федерация

Павел Карасев, Московский государственный университет, Российская Федерация

Андреас Кюн, Институт Восток-Запад, Соединенные Штаты Америки

Владимир Иванов, Институт Восток-Запад, Соединенные Штаты Америки

Энекен Тикк, Институт киберполитики, Эстония

Мика Керттунен, Институт киберполитики, Финляндия

Дэниэл Штауффахер, Фонд «ИКТ для мира», Швейцария

ISBN 978-5-6044056-2-8

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Окинавская декларация 2000 года о формировании глобального информационного общества ознаменовала начало новой эры развития человечества. Эта эра характеризуется интенсивным развитием глобальной информационной среды информационно-коммуникационных технологий (ИКТ-среды), основу которой составляет глобальная информационная инфраструктура. ИКТ-среда приобрела черты нового пространства реализации общественных отношений. Данное обстоятельство создает реальные возможности как для повышения качества жизни человека, устойчивого развития общества, так и для усиления международной напряженности, возникновения угрозы нарушения международного мира и безопасности. Возрастает опасность враждебного использования ИКТ в военно-политических целях. Увеличивается количество способов их возможного использования для оказания «силового» воздействия на противостоящую сторону.

Российская Федерация, как и многие другие страны, неизменно выступает за создание системы обеспечения международной информационной безопасности, нацеленной на предотвращение «враждебного» использования ИКТ в качестве средства разрешения межгосударственных противоречий. С этой целью Российская Федерация стала инициатором создания нескольких групп правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (далее — ГПЭ). Практическая полезность этих инициатив сейчас осознается всеми государствами мира.

Усилиями правительственных экспертов ООН, которые в 2003 году приступили к изучению потенциальной опасности угроз международному миру и безопасности в области использования ИКТ, в 2010, 2013 и 2015 годах, были подготовлены и приняты консенсусом доклады Генеральному Секретарю ООН. В докладе ГПЭ 2015 года впервые сформулированы рекомендации по нормам, правилам и принципам ответственного поведения государств в ИКТ-среде.

С принятием на 73-ей сессии Генеральной Ассамблеей ООН проекта российской резолюции, закрепляющей эти рекомендации ГПЭ в качестве норм «мягкого» права[1], особую актуальность приобретает проблема их практического применения. В условиях обострения международной обстановки эксперты многих государств мира полагают, что разработка конкретных рекомендаций по практическому применению норм, правил и принципов ответственного поведения государств в ИКТ-среде могла бы способствовать снижению опасности возникновения конфликтов, обусловленных «враждебным» и злонамеренным использованием ИКТ государствами.

Не вызывает сомнения, что международные отношения в области использования ИКТ должны регулироваться международным правом. В то же время среди государств не существует единого мнения относительно того как именно и до какой степени международное право может быть применимо к отношениям в ИКТ-среде.

В связи с этим, представляется исключительно своевременной инициатива участников Международного исследовательского консорциума информационной безопасности (МИКИБ), выдвинутая в апреле 2018 года на международном Форуме в г. Гармиш-Партенкирхен (Германия). Участники Консорциума предложили образовать международную группу экспертов для обсуждения методологических трудностей и разработки общих подходов к оценке применимости норм, правил и принципов ответственного поведения государств в целях создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. В состав группы вошли эксперты, представляющие заинтересованные организации Российской Федерации, США, Эстонии, Южной Кореи и Швейцарии.

Мы уверены, что потенциал российских экспертов, изучающих проблемы формирования системы международной информационной без-

1 Резолюция ГА ООН (A/RES/73/27) от 5 декабря 2018 г.

опасности и, в частности, практического применения норм, правил и принципов ответственного поведения государств в ИКТ-среде, существенно увеличился с образованием в 2018 году Национальной Ассоциации международной информационной безопасности. Одним из важных направлений деятельности Ассоциации является проработка в упреждающем режиме проблем обеспечения международной информационной безопасности. Исходя из этого, Ассоциация прилагает усилия по содействию организации исследования проблем практического применения норм, принципов и правил ответственного поведения государств в ИКТ-среде, проводимых в рамках проекта Международного консорциума.

Я рад предложить вниманию читателя материалы Отчета международной группы экспертов о результатах ее работы в 2018–2019 годах, которые, несомненно, заслуживают внимательного изучения и обсуждения.

Президент Национальной ассоциации международной информационной безопасности

Председатель Международного исследовательского консорциума информационной безопасности

Владислав Шерстюк

РЕЗЮМЕ

По предложению Международного исследовательского консорциума по информационной безопасности международная группа экспертов в составе представителей Московского государственного университета имени М.В. Ломоносова, представленного Институтом проблем информационной безопасности (Российская Федерация), Центра киберправа Университета Коре (Корея), Фонда ИКТ для мира (Швейцария), Института киберполитики (Эстония) и Института Восток-Запад (Соединенные Штаты Америки) провела исследование проблем применения норм, правил и принципов ответственного поведения государств в ИКТ-среде, предложенных ГПЭ ООН (2014–2015 г.) и получивших приветствие Генеральной Ассамблеи ООН (A/73/27).

ГПЭ ООН в Докладе 2015 г. отметила, что рекомендации относительно добровольных, необязательных норм, правил и принципов (далее — рекомендации) по ответственному поведению государств будут способствовать поддержанию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. В настоящем исследовании изучено понятие ИКТ-среды, ее отличительные особенности и требуемые качества. Важно, что в этом исследовании рассматривается взаимосвязь между этими рекомендациями и международным правом, и делается вывод о том, что рекомендации в силу своего существования и перспектив применения способствуют развитию международного права. Они заполняют пробел, существующий в нынешнем дискурсе, продвигая методологический, а не идеологический подход к вопросу об ответственном поведении государств в ИКТ-среде.

Настоящее исследование показывает, что такие субъекты обеспечения международной информационной безопасности, как Соединенные Штаты Америки и Российская Федерация, могут найти общие позиции в вопросах сущности и важности таких ключевых понятий и институтов международного права как суверенитет государств в ИКТ-среде, права человека или международное право. Государства имеют разногласия в вопросе о применении этих концепций к международным отношениям как в ИКТ-среде («онлайн»), так и в традиционных пространствах («оффлайн»).

Соответственно, настоящее исследование предлагает подход к снижению остроты таких разногласий и методологический подход к формированию условий для применения рекомендаций ГПЭ ООН на основе взаимопонимания. Это создает основу для открытых дискуссий по поводу конкретных проблем международной информационной безопасности (кибербезопасности), предлагаемых решений и ожидаемого эффекта от их реализации. При этом, предлагаемая методология базируется на принципах международного права в международной информационной безопасности (кибербезопасности).

Это открывает перспективу продуктивного обсуждения конкретных правил, стандартов и других мер, которые необходимо будет создать для обеспечения практического применения международного права к рассматриваемым международным отношениям.

Цель международной группы экспертов заключалась в поиске методологического подхода к решению проблем обеспечения международной информационной безопасности (кибербезопасности) на основе создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

Авторы исследования рассмотрели возможность практического использования предлагаемой ими методологии на трех конкретных рекомендациях Параграфа 13 (g), (h) и (k) Доклада ГПЭ ООН 2015 года. Для каждой рекомендации в исследовании выделены специфические проблемы, связанные с их реализацией.

I. ВВЕДЕНИЕ

Настоящее исследование направлено на изучение проблем применения норм, правил и принципов ответственного поведения государств, способствующих поддержанию открытой, безопасной, стабильной, доступной и мирной среды информационно-коммуникационных технологий (ИКТ-среды)[2]. В соответствии с решением Международного исследовательского консорциума информационной безопасности от 14 апреля 2018 г. (г. Гармиш-Партенкирхен, Германия) в качестве непосредственного объекта изучения выбраны пункты (g), (h) и (k) параграфа 13 *Доклада Группы правительственных экспертов в области информатизации и телекоммуникаций в контексте международной безопасности ООН (2015 г.)* (далее – ГПЭ ООН).

В рамках исследования предложен методологический подход к оценке применимости международного права к международным отношениям в ИКТ-среде и сформулированы проблемы практического применения государствами рекомендаций по ответственному поведению в ИКТ-среде. В отчете о результатах настоящего исследования изложена также позиция участников проекта по интерпретации понятия «ИКТ-среда» как пространства международного сотрудничества.

Предлагаемая интерпретация базируется на предположении о том, что рекомендации по ответственному поведению государств в ИКТ-среде осуществляются, прежде всего на основе национального законодательства и в рамках национальной юрисдикции. В исследовании рассматриваются проблемы практического применения данных рекомендаций для регулирования международных отношений в ИКТ-среде.

Методологический подход, предложенный в настоящем исследовании, позволяет выяснить условия, при которых может быть достигнуто общее мнение экспертов по вопросу применения изучаемых рекомендаций ГПЭ ООН, содействующих созданию открытой, безопасной, стабильной, мирной и доступной ИКТ-среды.

Отчет будет полезен для ученых и специалистов, занимающихся проблемами международной и национальной информационной безопасности (кибербезопасности). Материалы отчета могут быть использованы при решении проблем эффективного использования потенциала суверенитета государств в ИКТ-среде для обеспечения их устойчивого развития, при разработке международных и национальных документов, определяющих соответствующую стратегию и политику.

Участники исследования не стремились представить согласованный отчет. Целью участников было определение наиболее критичных проблем и разногласий, препятствующих прогрессу в развитии и внедрении рекомендаций по ответственному поведению государств в ИКТ-среде. Многочисленные положения этого отчета сопровождаются замечаниями, показывающими в общих чертах различия во взглядах и интерпретациях, проявившихся в ходе обсуждений. Другие положения, будучи на этом этапе единодушными, могут вызвать разногласия в будущем на более глубоких уровнях детализации обсуждений. Эту исследовательскую работу участники рассматривают как отправную точку для мультидисциплинарного процесса, способного привлечь ученых и практиков, работающих в разнообразных плоскостях проблемы: разработчиков стратегии и планов обеспечения безопасности, следователей, адвокатов, дипломатов и операторов ИКТ.

Целью проведенного исследования являлось также определение проблем, нерешенность которых способствует сохранению различий в позициях государств по вопросам практического

2 В данном исследовании ИКТ-среда рассматривается, прежде всего, как развивающаяся совокупность национальных, международных и глобальных систем ИКТ, используемых для оказания услуг и размещения информационных систем. В то же время, в контексте возможного последующего исследования вопросов применения принципа «невмешательства во внутренние дела других государств» к международным отношениям в ИКТ-среде (A/70/174 n.26) представляется важным отметить, что ИКТ являются не только средством формирования информационных систем, но и активно используются для автоматизации формирования и рассылки контента потребителям.

применения добровольных, необязательных рекомендаций по ответственному поведению государств в ИКТ-среде. В рамках исследования также рассматриваются приоритетные направления развития этих рекомендаций с целью создания открытой, безопасной, стабильной, мирной и доступной среды ИКТ

В настоящее время позиции экспертов существенно расходятся в оценках возможности применения международного права для регулирования международных отношений в ИКТ-среде. Это неизбежно скажется на способах имплементации рекомендаций ГПЭ ООН и эффективности их практического применения. Надеемся, что изучение трудностей в понимании предмета правового регулирования и объективных трудностей в применении международного права к международным отношениям в ИКТ-среде сможет способствовать укреплению взаимопонимания и формирования атмосферы доверия между государствами в этой новой области международных отношений.

С этой точки зрения материалы отчета могут содействовать активизации дискуссий между специалистами в области международной информационной безопасности[3] (кибербезопасности[4]) по проблемам предотвращения злонамеренного и враждебного использования ИКТ, способного вызвать международные конфликты, усиление угроз международному миру и безопасности.

---

3 "Международная информационная безопасность" - состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества в области обеспечения международной информационной безопасности. Екатеринбург. 16 июня 2009 г. . - http://base.garant.ru/2571379/

4 This National Cyber Strategy outlines how we will (1) defend the homeland by protecting networks, systems, functions, and data; (2) promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; (3) preserve peace and security by strengthening the United States' ability — in concert with allies and partners — to deter and if necessary punish those who use cyber tools for malicious purposes; and (4) expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet. National Cyber Strategy of the United states of the America. September 2018.

ЧАСТЬ I

II. ОБЩАЯ ПОСТАНОВКА ПРОБЛЕМЫ ИССЛЕДОВАНИЯ И ОБОСНОВАНИЕ НЕОБХОДИМОСТИ ВЫРАБОТКИ МЕТОДОЛОГИЧЕСКОГО ПОДХОДА

1. Интенсивное и широкое использование ИКТ во всех сферах общественной и частной жизни создало условия для формирования и развития глобального информационного общества[5]. Общепризнано, что доверие к ИКТ и зависимость от них порождают не только позитивные возможности прогрессивного развития общества, но и серьезные угрозы национальной и международной безопасности.

2. Международная безопасность может трактоваться как состояние международных отношений, в котором на основе международного права созданы необходимые условия для соблюдения прав человека и устойчивого развития суверенных государств в экономической, социальной, политической и культурной сферах, поддерживается необходимый уровень защищенности природы. Обеспечение безопасности критических инфраструктур и, в том числе, информационных, посредством применения международного права и национальной правоприменительной практики будет способствовать устойчивому развитию общества.

3. Для изучения угроз в области информационной безопасности и разработки международных концепций обеспечения информационной безопасности Генеральный секретарь ООН собирал несколько Групп правительственных экспертов (далее ГПЭ, а также Группа) в области информатизации и коммуникаций в контексте международной безопасности[6]. ГПЭ ООН было поручено предложить меры по усилению безопасности глобальных систем информации и связи. Три из пяти ГПЭ ООН подготовили соответствующие доклады[7].

4. Доклады ГПЭ ООН отразили состояние проблемы обеспечения международной безопасности в отношении использования ИКТ государствами. ГПЭ ООН выделили ряд проблем в данных международных отношениях, в разрешении которых применение и развитие рекомендаций по ответственному поведению государств может иметь существенное значение. В докладах ГПЭ ООН обозначены существующие и потенциальные угрозы международному миру и безопасности, для противодействия которым могут быть применены рекомендации по ответственному поведению государств в целях создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды, а также содержатся предложения по направлениям сотрудничества государств в данной области.

5. Наиболее детальные рекомендации по ответственному поведению государств в ИКТ-среде сформулированы в Докладе ГПЭ ООН 2015 г.[8]. Группа попросила государства-члены ООН «внимательно изучить предлагаемые рекомендации и проанализировать возможные пути их доработки и осуществления»[9].

6. Попытка развития рекомендаций, содержащихся в Докладе ГПЭ ООН 2015 г., предпринятая следующей ГПЭ ООН в 2016-2017 гг., не привела к ожидаемым результатам. Эксперты не смогли согласовать позиции по вопросу о применении международного права к использованию ИКТ государствами и подготовить со-

5 Окинавская хартия глобального информационного общества. 22 июля 2000 г.. Окинава. Япония.
6 2003-2004, 2009-2010, 2012-2013, 2014-2015, 2016-2017.
7 Доклады 2010, 2013 и 2015 гг. ГПЭ ООН в области информатизации, коммуникации в контексте международной безопасности (A/65/201, A/68/98, A/70/174)*
8 Резюме по Докладу ГПЭ ООН, 2015. A/70/174
9 Summary of Document A/70/174

гласованный доклад о результатах работы[10]. В соответствии с резолюциями 73-й сессии ГА ООН изучение вопросов применения и развития рекомендаций по ответственному поведению государств в ИКТ-среде в 2019–2021 гг. осуществляют две группы экспертов: Группа ООН открытого состава[11] и ГПЭ ООН на основе справедливого географического представительства[12].

7. В докладах ГПЭ ООН, работавших в 2013 и 2015 гг., отмечено, что «международное право, и, в частности, Устав Организации Объединенных Наций, применимо к международным отношениям в ИКТ-среде и имеет важное значение для поддержания мира и стабильности и создания открытой, безопасной, мирной и доступной информационной среды»[13]. Кроме того, отмечена «важность международного права, Устава ООН и принципа суверенитета в качестве основы для повышения безопасности в сфере использования ИКТ государствами» [14]. Данные положения одобрены в резолюциях ГА ООН, которая приветствовала отчеты ГПЭ ООН (2013 г., 2015 г.). Данная позиция поддержана также в заявлениях и коммюнике G7, G20, НАТО, ЕС, ШОС и БРИКС[15].

8. Как следует из материалов многочисленных конференций и семинаров по вопросам обеспечения международной информационной безопасности (кибербезопасности)[16], в международном экспертном сообществе практически отсутствует общее понимание того, как именно должно применяться международное право для противодействия угрозам международной и национальной безопасности государств в ИКТ-среде. Отсутствует также согласие экспертного сообщества в вопросе источников международного права в области противодействия угрозам международному миру и безопасности, возникающим вследствие тенденции развития и использования ИКТ в военно-политических целях. Имеются существенные различия во взглядах экспертов и на роль ГПЭ ООН в вопросе прогрессивного развития соответствующих отраслей международного права.

9. В докладе ГПЭ ООН (2015 г.) не определено соотношение между рекомендациями в области ответственного поведения государств и международным правом[17]. В этих условиях представляется важной разработка транспарантных и конструктивных подходов к анализу практической применимости рекомендаций по ответственному поведению государств для создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды, для достижения устойчивого и ориентированного на мир и безопасность развития ИКТ.

10. В связи с изложенным, а также с повышением влияния развития ИКТ на формирование глобального информационного общества, эффективная работа в 2019–2021 гг. обеих групп экспертов ООН приобретает особое значение. В соответствии с мандатами групп им поручено определить потребность в дальнейшем развитии рекомендаций по ответственному поведению государств в ИКТ-среде и в этом контексте выделить направления развития или адаптации международного права.

11. Многие государства и специалисты исходят из того, что возникновение глобальной ИКТ-среды создало новое измерение в раз-

10 Krutskikh A., Streltsov A.. International information security: problems and ways of resolving them. Forthcoming in Tikk, E. and Kerttunen, M. (editors) Routledge Handbook of International Cybersecurity. Routledge, 2020.

*11 ГА ООН. A/C.1/73.1/L.27**

12 ГА ООН. A/C.1/73.1/L 37

13 ГА ООН. A/68/98, п.19*

14 ГА ООН. A/70/174

15 Циндаоская декларация Совета глав-государств ШОС от 18 июня 2018 г., Йоханнесбургская декларация десятого саммита БРИКС. 26 июля 2018 г.

16 TikkE., M.Kerttunen, Cyber treaty is coming. Что делать? Cyber policy institute. 2018

17 Более детальную информацию можно найти в: Крутских А.В.: миру навязывается концепция военных мер в цифровой сфере. http://russkoepole.de/ru/news-18/3913-v-krutskikh-miru-navyazyvaetsya-kontseptsiya-voennykh-mer-v-tsifrovoj-sfere.html ; Tikk & Kerttunen, Parabasis: International cyber-diplomacy in stalemate. Norwegian Institute of International Affairs (October 2018).

витии международных отношений и, соответственно, — новое пространство применения международного права[18]. При этом обозначились существенные различия в интерпретации международного права[19]. Относительная новизна проблем безопасности ИКТ-среды стала причиной возникновения вопросов о юридической определенности спорных ситуаций в ИКТ-среде и снизила предсказуемость поведения государств в этих ситуациях.

12. Различия в подходах к применению международного права для регулирования международных отношений в ИКТ-среде наглядно проявляются как в позициях национальных государств, так и экспертов. Предыдущие исследования проблем применения рекомендаций по ответственному поведению государств в целях создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды выявили различия как в понимании проблемы, так и в предлагаемых подходах к ее решению[20]. Определенные методологические трудности проявились в Таллиннском руководстве по применению международного права к «кибероперациям»[21]. Данное исследование позиционируется некоторыми политиками и экспертами в качестве основного источника знаний о порядке применения международного права к проблемам кибербезопасности. Политические противоречия между государствами в вопросе о применимости международного права наглядно проявляются при обсуждении проблем обеспечения международной информационной безопасности и кибербезопасности в ходе работы ГПЭ ООН 2016–2017 гг[22]. В этой дискуссии у экспертов отсутствует общее понимание природы возникающих проблем применения международного права к международным отношениям в ИКТ-среде.

13. В настоящее время рекомендации ответственного поведения государств в ИКТ-среде, получившие приветствие от ГА ООН[23] de facto не применяются государствами и, с этой точки зрения, еще, в полной мере, не оказывают соответствующего регулирующего воздействия на международные отношения. Можно предположить, что со временем, посредством практики государств, рекомендации по ответственному поведению, скорее всего, станут полноправной составляющей «мягкого» международного права. Несмотря на то, что принятие норм «мягкого права» не создает непосредственных юридических обязательств для государств и, соответственно, их несоблюдение не порождает международной правовой ответственности государств, это тем не менее дает возможность привлечь внимание международного сообщества к поведению государств в ИКТ-среде посредством использования информационной сферы. Как отметила ГПЭ ООН 2015 г. предложенные нормы отражают «ожидания международного сообщества» и определяют «стандарты ответственного поведения», применение которых «позволит международному сообществу оценить действия и намерения го-

18 Россия и информационная безопасность. Международная конференция. Москва, 20 декабря 2016 г. Международная жизнь. Специальный выпуск. 2017.

19 Крутских А.В., Стрельцов А.А.. Международное право и проблема обеспечения международной информационной безопасности. Международная жизнь. 2014, 11; Стрельцов А.А. Адаптация международного права к информационному пространству. Digital report. 27.04.2016; Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology A Commentary. Editor-in-Chief E. Tikk. Civil Society and Disarmament. Voluntary, UN. NY. 2017; State, business, civil society. Information Security. Materials of the 11th International Forum "Partnership of the State, Business and Civil Society at. Ensuring international information security. Supplement to the journal International Affairs. Garmisch-Partenkirchen, Germany, April 24-27, 2017

20 Стрельцов А.А. Рекомендации в отношении правил и принципов ответственного поведения государств по обеспечению открытой, безопасной и мирной ИКТ-среды. Digital report. 28.04.2016; Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology A Commentary. Editor-in-Chief E. Tikk. Civil Society and Disarmament. Voluntary, UN. NY. 2017; State, business, civil society. Information Security. Materials of the 11th International Forum "Partnership of the State, Business and Civil Society at. Ensuring international information security. Supplement to the journal International Affairs. Garmisch-Partenkirchen, Germany, April 24-27, 2017

21 Michael N. Schmitt, Tallinn Manual of International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2015).

22 A/72/327

23 A/73/505 от 19.11.2018

сударств»[24]. Можно ожидать, что постепенно эти рекомендации по ответственному поведению государств приобретут de facto статус норм международного права или, возможно, обычного международного права.

14. В настоящем исследовании изучение проблем правового регулирования международных отношений в области применения рекомендаций по ответственному поведению государств в ИКТ-среде носит в основном теоретический характер и основано на гипотетических сценариях.

15. Данное исследование направлено на выявление способов лучшего понимания проблем правового регулирования международных отношений в ИКТ-среде и обсуждение возможных направлений развития рекомендаций по ответственному поведению государств в ИКТ-среде. Исследование так же призвано определить направления развития международного права, создающие условия для правового регулирования соответствующих отношений. В исследовании предполагалось лишь обозначить проблемы применения международного права к ИКТ-среде и содействовать поиску вариантов их решения.

16. Для достижения целей исследования важно сформулировать общий подход к оценке применимости рекомендаций по ответственному поведению государств в ИКТ-среде для регулирования международных отношений. Предполагается, что применимость этих рекомендаций характеризуется, прежде всего, следующим: a) возможностью применения этих рекомендаций государствами на основе норм и принципов международного права, включая практику государств в использовании средств мирного разрешения международных споров; b) возможностью применения этих рекомендаций уполномоченными международными организациями и учреждениями для содействия разрешению международных споров, являющихся результатом инцидентов в ИКТ-среде.

17. Можно полагать, что сближение позиций национальных государств и позиций международного экспертного сообщества по вопросам применения добровольных и необязательных рекомендаций по ответственному поведению государств будет содействовать успешному поиску средств противодействия угрозам международному миру и безопасности, предотвращению кризисов и конфликтов, обусловленных инцидентами в ИКТ-среде. Это будет способствовать также использованию ИКТ для развития глобальной экономики национальных обществ. Большее согласие могло бы способствовать предотвращению возникновения недоразумений и недопонимания в оценке ситуаций, связанных с применением ИКТ государствами для обеспечения национальной или международной безопасности. Настоящее исследование создает основу для обсуждения методологии изучения и применения добровольных, необязательных рекомендаций по ответственному поведению государств в ИКТ-среде[25].

18. В то время как основное внимание этого исследования сосредоточено на поведении государств и правовых последствиях деятельности государств в киберпространстве, обеспечение реального функционирования этого пространства требует сотрудничества множества негосударственных заинтересованных субъектов, включая частные компании, экспертов в области ИКТ, научные организации и организации гражданского общества. Так называемые «мультистэйкхолдинговые» или «многосторонние» подходы сами по себе не являются общепризнанными, поскольку некоторые полагают, что они противоречат суверенитету государств или их главной ответственности за обеспечение национальной и международной безопасности. В то же время

24 ГА ООН. A/70/174

25 Materials of the work of the Group of Governmental Experts on achievements in the field of information and telecommunications in the context of international security 2016-2017.

государство без сотрудничества с множеством участников этого процесса, которые владеют «ключевой» инфраструктурой сети Интернет и обслуживают ее, не может обеспечить безопасность его киберпространства. Для успешного применения международного права в киберпространстве потребуется участие этих субъектов, и возможность консультирования с ними относительно эффективности предложенных норм, политик и соглашений, в осуществлении которых они будут участвовать. В этой области уже существует много полезных процессов. Это способствует конструктивному развитию взаимопонимания, что и определяет ответственное поведение[26].

19. Для дальнейшего изучения проблем применения международного права Рабочей группе открытого состава ООН целесообразно активно привлекать специалистов в области международного права применительно к использованию ИКТ для обеспечения национальной и международной информационной безопасности (кибербезопасности), а также в области обеспечения функционирования ИКТ среды.

III. МЕТОДИЧЕСКИЕ ПОЛОЖЕНИЯ

20. Как было отмечено ранее, эксперты существенно расходятся в оценке правового содержания добровольных, необязательных рекомендаций по ответственному поведению государств в ИКТ-среде, а также в оценке возможности применения международного права к отношениям по поводу поведения государств в ИКТ-среде. С учетом этого, представляется важным достаточно четко определить структуру исследования и схему его проведения, обеспечивающих возможность сравнения позиций экспертов по рассматриваемым вопросам, выяснения причин возникновения и содержание разногласий в трактовке рекомендаций.

21. С этой целью в настоящем исследовании каждая изучаемая рекомендация рассматривается сначала контекстуально, а затем содержательно. В рамках контекстуального анализа определяются: область международных отношений, которая оказывает влияние на международную безопасность; группа международных отношений, на которую направлено воздействие рекомендации и цель этого воздействия, т.е. результат, который должен быть достигнут вследствие применения рекомендации. Соответственно, обсуждение каждой рекомендации следует за систематизированным уяснением вопросов о ее предмете, объекте и цели, сопровождается выявлением проблем применения этой рекомендации.

22. Данное исследование создает основу для инициирования дискуссии заинтересованных специалистов по содержанию выявленных проблем.

23. По каждой рекомендации авторы исследования изложили свою позицию в отношении подходов к решению вопросов применения. Эта часть исследования призвана привлечь внимание к практическим соображениям, которые участники реализации предложенных рекомендаций при желании могут дополнительно обсудить или прояснить.

26 Examples include the Global Commission on the Stability of Cyberspace (for which the EastWest Institute served as Secretariat) www.cyberstability.org, as well as Global Forum on Cyber Expertise (GFCE), World Summit on the Information Society (WSIS), the Global Commission on Internet Governance, the Internet Governance Forum (IGF), the Global Conference on CyberSpace (GCCS), the NETmundial Initiative, the Organization for Security and Co-operation in Europe (OSCE), the African Union Commission (AUC), the Charter of Trust, the Cybersecurity Tech Accord, the United Nations Institute for Disarmament Research (UNIDIR), the Paris Call for Trust and Security in Cyberspace, and the UN Secretary-General's High-level Panel on Digital Cooperation. The ICT4Peace Cybersecurity Policy and Diplomacy Capacity Building Program.

ЧАСТЬ II

IV. ОБЩИЕ ПРОБЛЕМЫ ПРИМЕНЕНИЯ МЕЖДУНАРОДНОГО ПРАВА К ИКТ-СРЕДЕ

IV.1. Роль государств в применении норм, правил и принципов ответственного поведения государств

24. В соответствии с пунктом b) параграфа 28 Доклада ГПЭ ООН 2015 г., «в процессе использования ИКТ государства должны соблюдать, наряду с другими принципами международного права, такие принципы, как государственный суверенитет, суверенное равенство, разрешение споров мирными средствами и невмешательство во внутренние дела других государств». Кроме того, «государственный суверенитет и международные нормы и принципы, вытекающие из принципа государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием ИКТ[27], а также на юрисдикцию государств над ИКТ-инфраструктурой на их территории»[28].

25. Данная глава посвящена рассмотрению вопроса о суверенитете государств в ИКТ-среде как предпосылки появления практики интерпретации содержания норм и принципов международного права к применению ИКТ государствами, а также имплементации рекомендаций по ответственному поведению государств. Авторы исходили из того, что несмотря на различия в политической интерпретации и практическом применении суверенитета государств в современной геополитической действительности[29] и особенно в контексте использования и развития ИКТ, понятие «суверенитет» остается фундаментальным общим знаменателем в дискуссии о применимости международного права к ИКТ-среде[30].

26. Государственный суверенитет заключается в верховенстве, единственности и независимости государственной власти как на территории своей страны, так и в отношениях с другими странами. В международных отношениях суверенитет государства проявляется в совокупности его прав и возможности применения силы в соответствии с принципами и нормами международного права, закрепленными в принятых им международных договорах, а также с международными правовыми обычаями, отражающими всеобщую практику. Суверенитет, в свою очередь, выражается в общих принципах права, принимаемых цивилизованными народами. В международных отношениях суверенитет проявляется, в частности, в принятии или не принятии на себя международных обязательств.

27. Территория государства образуется совокупностью физических сред, в пределах которых государство осуществляет суверенитет, т.е. применяет свое правовое верховенство и юрисдикцию. В состав государственной территории входят суша с ее недрами, водная территория (внутренние воды и территориальное море государства), а также воздушное пространство. Территория государ-

---

27 Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;149-ФЗ. 22 июля 2006 г.

"On Information, Information Technologies and Information Protection". ICT (information and communications technology – or technologies) is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning. ICTs are often spoken of in a particular context, such as ICTs in education, health care, or libraries. The term is somewhat more common outside of the United States. www.earchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies

28 A/68/98, para 20.

29For example, see (1) https://www.comparativepolitics.org/jour/article/viewFile/123/139; and (2) https://www.japantimes.co.jp/opinion/2015/09/21/commentary/world-commentary/nature-sovereignty-key-issue-russia-u-s-divide/

30 «Государственный суверенитет – свойство государства самостоятельно и независимо от власти других государств осуществлять свои функции на своей территории и за ее пределами, в международном общении». Козлова Е.И., Кутафин О.Е.. Конституционное право. М., Юристъ. 2004, стр.165;

«Perhaps the outstanding characteristic of a state is its independence, or sovereignty. This was defined in the Draft Declaration on the Rights and Duties of States prepared in 1949 by the International Law Commission as

the capacity of a state to provide for its own well-being and development free from the domination of other states, providing it does not impair or violate their legitimate rights.» Malcolm N. Shaw. International law. Cambridge. University press. N.Y., 2008. p. 211

ства имеет признанные другими государствами границы. Признание границ государства достигается посредством заключения соответствующих договоров с соседними государствами, а также официальных заявлений по данному вопросу уполномоченных органов других государств.

28. Объектом суверенитета в контексте данного анализа является ИКТ-среда. Как отмечено в Докладе ГПЭ ООН 2015 г., целью работы ГПЭ ООН является создание открытой, безопасной, стабильной, доступной и мирной ИКТ-среды[31].

29. Достижение международного единодушия в практическом применении государственного суверенитета в ИКТ-среде требует общего понимания природы существующих разногласий между государствами по этому вопросу с ясным выделением политических и технических аспектов практического применения суверенитета и определения границ юрисдикции в сфере ИКТ.

Ремарка. Мнения участников исследовательского проекта относительно содержания политических разногласий разошлись. По мнению одних участников проекта причиной разногласий является, прежде всего, сосредоточенность некоторых государств на таких вопросах как применение юрисдикции к ключевым элементам системы управления сетью Интернет, на «враждебном» и «вредоносном» использовании ИКТ для решения межгосударственных противоречий, на использовании для этого частных компаний, так же как на злоупотреблении свободой информации для распространения недостоверной информации. По мнению других участников проекта, причиной разногласий являются сосредоточенность некоторых государств на чрезмерном регулировании отношений в области ограничения свободы информации.

IV.2. Определение ИКТ-среды

30. В российской политической доктрине понятие «ИКТ-среда» является синонимом понятия «информационная сфера», которое раскрывается как «совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений» [32].

31. В политической доктрине США близким аналогом понятия «ИКТ-среда» является понятие «информационная среда», которое раскрывается как «совокупность индивидов, организаций и систем сбора, обработки, распространения и использования информации» [33].

32. С точки зрения физической природы процессов, протекающих в ИКТ-среде, ИКТ-среда представляет собой «киберпространство», которое в политической доктрине США рассматривается как «глобальная область информационной сферы, включающая взаимосвязанные сети инфраструктур информационных технологий и расположенные в данных сетях, включая Интернет, телекоммуникационные сети, компьютерные системы, содержащие процессоры и контроллеры»[34].

33. Важной составляющей ИКТ-среды является информационная инфраструктура, которая создает условия для автоматизированной обработки информации (в частности, ее производства или хранения) и коммуникации (получения, передачи и распространения) дан-

31 p. 1, A/70/174.

32 Доктрина информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 5 декабря 2016 г., № 646

33 US Department of Defense, DOD Dictionary of Military and Associated Terms (JP 1-02) (June 2019), and Strategy for Operations in the Information Environment, (June 2016). The latter explains (p. 3) the notion of Information Environment as a heterogeneous global environment where humans and automated systems observe, orient, decide, and act on data, information, and knowledge. With its function as a conduit for in uence on decision-making and command and control, the IE is a key component of the commander's operational environment. Characterized by ubiquitous on-demand media and interpersonal hyper-connectivity, today's IE enables collaboration and information sharing on an unprecedented scale."

34 US Department of Defense, DOD Dictionary of Military and Associated Terms (JP 1-02) (June 2019).

ных в различных сферах жизнедеятельности общества[35].

IV.3. Особенности ИКТ-среды

34. Важными чертами ИКТ-среды, которые отличают ее от традиционных пространств поддержания дружественных и мирных международных отношений, являются: глобальность ИКТ-среды, обусловленная зависимостью ее функционирования от заинтересованных граждан и организаций, находящихся в различных юрисдикциях[36], а также государств (большое число прямых и косвенных участников и заинтересованных сторон («стейкхолдеров»); искусственный характер ИКТ-среды, обусловленный интеграцией в ее составе вычислительных и коммуникационных устройств, систем и сетей, функционирующих на основе использования глобальной системы цифровых идентификаторов; многоуровневость системы открытых протоколов взаимодействия устройств и систем, реализуемых в вычислительных, коммуникационных и иных устройствах ИКТ. Данные технологии представляют собой совокупность методов, способов и алгоритмов обработки информации в вычислительных и коммуникационных устройствах, системах, сетях.

35. Важным следствием искусственности, цифрового характера и распределенной структуры ИКТ-среды являются трудности наблюдения и объективной регистрации процессов использования ИКТ. Доступ к публичным и частным системам, возможность целенаправленного распространения информации позволяют государствам оказывать влияние и осуществлять контроль процессов социально-политического развития общества, а ненаблюдаемость этого процесса — отрицать противоправное вмешательство во внутренние дела других государств[37]. Такое вмешательство способно нарушить национальную безопасность, региональный и международный мир, безопасность и стабильность.

36. Трудности наблюдения за процессом использования ИКТ государствами существенно усложняют обнаружение и установление причинно-следственных связей между действиями государств и их последствиями, а также оценку реальных и ожидаемых последствий таких действий. Этим обстоятельством может быть объяснена появляющаяся практика непредоставления фактов, подтверждающих обоснованность приписывания «государствами – жертвами»[38] ответственности государствам, предположительно спонсирующим кибератаки и доказательств существования объективной связи между инцидентом в ИКТ-среде и действиями государства, которому приписывается ответственность за этот инцидент.

37. Виртуальный характер процессов в ИКТ-среде в совокупности с ограниченными возможностями национальных уполномоченных органов в объективном, юридически надежном анализе и обнаружении инцидентов в ИКТ-среде, делает атрибуцию весьма трудной задачей. Трудности в объективной, юридически надежной фиксации инцидентов в ИКТ-среде могут привести к политизированным предположениям о возможных сторонах этих инцидентов и мотивах соответ-

35 Информационная инфраструктура — система организационных структур, подсистем, обеспечивающих функционирование и развитие информационного пространства страны и средств информационного взаимодействия. Включает в себя: совокупность информационных центров, подсистем, банков данных и знаний, систем связи, центров управления, аппаратно-программных средств и технологий обеспечения сбора, хранения, обработки и передачи информации. Обеспечивает доступ потребителей к информационным ресурсам. https://kartaslov.ru/

36 For further discussion of this broader communities, see paragraph [#18#] above.

37 On soft law in this field, see for example, UNGA, "Respect for the principles of national sovereignty and non-interference in the internal affairs of States in their electoral processes", A/44/147 (15 December, 1989).

38 «Государство – жертва» - государство, которое заявляет о причинении ему существенного ущерба в результате «кибернападения» на объекты его информационной инфраструктуры.

ствующих действий[39]. Это создает существенные проблемы в применении государствами международного права к международным отношениям в ИКТ-среде.

38. Ненаблюдаемость процессов использования государствами ИКТ усложняет оценку предполагаемого ущерба от опасных действий в этой области. В свою очередь, данное обстоятельство затрудняет правовую оценку действий государств в области ИКТ, которые создают предпосылки для возникновения угроз международному миру и безопасности.

39. С учетом изложенного можно полагать, что ИКТ-среда как объект международного права представляет собой юридическую фикцию. Данная фикция заключается в приписывании ИКТ-среде свойств традиционной территории государства и распространении на нее государственного суверенитета.

40. Недостаточная изученность вопросов применения международного права для регулирования отношений в ИКТ-среде обусловливает необходимость обсуждения следующих проблем: a) содержание международных обязательств государств в ИКТ-среде; b) правовое закрепление пространственных пределов суверенитета государств в ИКТ-среде; c) определение вопросов, входящих в национальную юрисдикцию.

IV.4. Требуемые качества ИКТ-среды

41. Три ГПЭ ООН, работавшие в 2009–2010, 2012–2013 и 2014–2015 гг., подчеркнули, что ИКТ-среда должна быть открытой, безопасной, стабильной, доступной и мирной. Достижение этих качеств должно явиться результатом, в том числе применения государствами, международными организациями и институтами рекомендаций по ответственному поведению государств в ИКТ-среде. Для оценки текущего состояния «открытости», «безопасности», «стабильности», «доступности» и «мирности» ИКТ-среды представляется важным определить содержание этих качеств.

42. Учитывая, что данные понятия могут раскрываться по-разному, ниже предлагается один из возможных подходов к решению данной задачи.

43. Открытость ИКТ-среды заключается в возможности ее использования людьми, проживающими во всех государствах мира, посредством предоставления доступа населения к глобальным информационным ресурсам и через национальные ИКТ-среды — к глобальной ИКТ-среде.

44. Безопасность ИКТ-среды заключается в способности государств, организаций и индивидов, создающих, развивающих и использующих информационную инфраструктуру и соответствующие службы, предотвращать угрозы безопасности прав и свобод человека, организаций и национальной безопасности, противодействовать этим угрозам, а также поддерживать функционирование служб, содействовать поддержанию международной безопасности и мира.

45. Стабильность заключается в способности ИКТ-среды обеспечивать выполнение задач развития и функционирования информационной инфраструктуры, а также поддержание устойчивого функционирования национальных и глобальной информационных сфер в условиях нарушения работоспособности отдельных элементов инфраструктуры.

46. Доступность заключается в постоянной готовности ИКТ-среды к удовлетворению законных интересов, реализации прав и выполнения обязанностей субъектов жизнедеятельности общества (человека, коммерческих и некоммерческих организаций, органов государственной власти), к предоставлению услуг автоматизации обработки и коммуникации информации, доступа к информации.

47. Мирность заключается в способности ИКТ-среды содействовать стабильному развитию общества, мирному разрешению международных споров таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость[40], не допускать угрозы

39 Kazakovtsev, A.V., NATO and Cybersecurity. News. Volgograd State University. Ser. 4, History. 2012, №2 (22).
40 Устав ООН. Ст. 2(3)

силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с Целями Объединенных Наций[41].

ЧАСТЬ III

V. ПРИМЕНЕНИЕ НОРМ, ПРАВИЛ И ПРИНЦИПОВ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ

48. В данном разделе представлены результаты обсуждений между участниками проекта по практическому применению рекомендаций (g), (h) и (k) параграфа 13 Доклада Группы правительственных экспертов в области информатизации и телекоммуникаций в контексте международной безопасности ООН (2015 г.).

49. В процессе обсуждения рассматривались нормы и принципы международного права, которые авторы признали применимыми к исследуемым рекомендациям.

50. Нормы и принципы международного права, рассмотренные участниками проекта, не исчерпывают множество норм и принципов, содержащихся в источниках международного права, которые можно было бы применить для регулирования рассматриваемых групп международных отношений.

51. Полученные результаты иллюстрируют возможные политико-правовые последствия нерешенности проблем, указанных в разделе II, для реализации межгосударственных отношений на основе международного права.

52. При рассмотрении выводов и рекомендаций, сформулированных авторами, необходимо учитывать следующее: a) существующее международное право создавалось для упорядочения отношений между суверенными и равными государствами; b) межгосударственные отношения в ИКТ-среде складываются по поводу как объектов нематериального мира (информации, ИКТ, информационной и коммуникационной деятельности), так и материальных объектов (устройств, систем и сетей связи), а также по поводу поведения человека в этих сферах, пространствах и средах, существенно отличающегося с точки зрения применения средств правового воздействия от материального мира.

53. Надеемся, что выводы и рекомендации, предлагаемые авторами, будут способствовать развитию дискуссии по вопросам применения и развития международного права.

V.1. Параграф 13 g) доклада ГПЭ ООН 2015 г.

Предмет, объект и цель[42] рекомендаций

54. В соответствии с параграфом 13 g) доклада ГПЭ ООН 2015 г. «Государства должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции».

55. Генеральная Ассамблея ООН отметила необходимость усиления «связей между важнейшими инфраструктурами, в том числе критическими, стран и информационной инфраструктурой, которые во все большей степени обеспечивают взаимосвязанность функционирования важнейших инфраструктур и влияют на них»[43].

---

41 Там же. Ст. 2(4)

42 Предмет рекомендаций – область межгосударственных отношений, имеющая существенное значение для создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

Объект рекомендаций – группа межгосударственных отношений, на регулирование которых направлено правовое воздействие необязательных, добровольных норм, правил и принципов ответственного поведения государств;

Цель рекомендаций – создание правовых условий, обеспечивающих желательное поведение государств в отношениях, состоящих объект рекомендаций.

43 Создание глобальной культуры кибербезопасности и защиты важнейших информационных инфраструктур. Резолюция ГА ООН, A/RES/58/199

56. ГПЭ ООН выявила тревожные тенденции «в глобальной ИКТ-среде, включая резкое увеличение числа случаев злонамеренного использования ИКТ государственными и негосударственными субъектами». Это «создает угрозу для всех государств» и может «нанести ущерб международному миру и безопасности»[44]. По мнению правительственных экспертов, «многие государства занимаются наращиванием потенциала в сфере ИКТ в военных целях» и, вследствие этого, «использование ИКТ в будущих конфликтах между государствами становится более вероятным»[45]. «К числу наиболее пагубных нападений с использованием ИКТ относятся нападения на критически важные объекты инфраструктуры и связанные с ними информационные системы государств. Опасность вредоносных нападений с использованием ИКТ на критически важную инфраструктуру является реальной и серьезной»[46]. Не меньшие опасения у ГПЭ ООН вызывает «использование ИКТ для террористических целей, в том числе для совершения террористических нападений на объекты ИКТ или связанную с ИКТ инфраструктуру, а не только для вербовки сторонников, финансирования, обучения и подстрекательства». Обращает на себя внимание и «многообразие злонамеренных негосударственных субъектов (включая преступные группировки и террористов)», которые, используя «различные мотивы, быстротечность злонамеренных нападений в сфере ИКТ, а также трудности, связанные с определением источника инцидента в сфере ИКТ, увеличивают существующую угрозу». «Государства с полным основанием обеспокоены опасностью дестабилизирующих последствий ошибочного понимания намерений другой стороны, потенциалом возникновения конфликта и возможностью нанесения ущерба их экономике»[47].

57. Изучаемая рекомендация ГПЭ ООН призывает к добровольному осуществлению государствами своего суверенитета и применения юрисдикции для обеспечения защиты критической инфраструктуры, а также информационной инфраструктуры, составляющей техническую основу критической инфраструктуры.

58. Предметом рекомендации являются международные отношения в области функционирования, устойчивости и безопасности информационной инфраструктуры. Для применения территориальной юрисдикции государств к информационной инфраструктуре необходимо: a) четко определить важную информационную инфраструктуру или инфраструктуру, имеющую для государств критическое значение; b) обеспечить ее функционирование, устойчивость и безопасность. Предполагается, что, обеспечивая адекватную защиту национальной критической инфраструктуры и национального сегмента критической информационной инфраструктуры, государства уменьшают угрозы международному миру и безопасности.

Ремарка. В российской концепции международной безопасности упоминается триада таких угроз как угрозы преступного, террористического и военно-политического характера. В американской концепции международной кибербезопасности основное внимание уделяется противодействию угрозам военного использования ИКТ, а также угрозам криминального и террористического характера как основной области применения права и обеспечения национальной безопасности в киберпространстве[48].

59. Объектом рекомендации являются международные отношения в области обеспечения безопасности и устойчивости функци-

44 Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. 22 июля 2015 г., A/70/174
45 A/70/174
46 A/70/174
47 A/70/174
48 International Strategy for Cyberspace, 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; Department of State International Cyberspace Policy Strategy, 2016, https://www.hsdl.org/?view&did=792759

онирования национальной критической инфраструктуры.

60. Цель рекомендации состоит в создании условий для достижения каждым государством достаточной степени национальной безопасности посредством предоставления правовых гарантий защиты функционирования критической инфраструктуры от «существующих и появляющихся угроз использования ИКТ государствами и негосударственными субъектами таким образом, который может подвергнуть опасности международный мир и безопасность»[49]. Данная рекомендация направлена на создание ситуации, в которой информационная инфраструктура и критическая инфраструктура других государств будут также адекватно защищены от выделенных угроз. Ожидается, что, посредством применения изучаемой рекомендации государства смогут привлечь внимание международного сообщества к последствиям, возникающим в случае нарушения функционирования, устойчивости или безопасности соответствующей инфраструктуры из-за несоответствующего уровня их безопасности, включая компенсации за вредные последствия возникновения таких обстоятельств.

61. Меры, принимаемые для защиты критической инфраструктуры и информационной инфраструктуры, находящейся под юрисдикцией государства, должны исходить из необходимости противодействия угрозам, отмеченным, в частности, в параграфах 4 - 7 Доклада ГПЭ ООН 2015 г.

Возможные направления обсуждения имплементации рекомендации

62. Исходя из того, что государства должны обеспечить защиту своей критической инфраструктуры, а также информационной инфраструктуры, находящихся под их юрисдикцией, изучаемая рекомендация может быть имплементирована в международное и национальное право, политику и стратегию. Имплементация может быть направлена на создание условий для взаимодействия всех заинтересованных сторон на национальных и международном уровнях.

63. В международном праве созданы некоторые механизмы, которые могут быть применены к защите критических областей, объектов, функций и услуг[50].

64. Соответствующие меры по защите критической информационной инфраструктуры могут включать, *inter alia*, действия по выявлению угрозы, уменьшению уязвимости критической информационной инфраструктуры, минимизации ущерба и времени восстановления в случае нанесения ущерба или попыток нарушения защиты, а также действия по выявлению угрозы или источников таких попыток, эффективность которых может быть увеличена, например, посредством обмена информацией о лучших практиках и проведения консультаций, оказания помощи и других форм сотрудничества.

65. Международное сотрудничество государств, связанное с применением комментируемой рекомендации, может содействовать успешной реализации национальных стратегий снижения риска для защищаемых критической инфраструктуры и информационной инфраструктуры, находящихся под национальной юрисдикцией. Данное сотрудничество может предусматривать[51]:

a) доступность сетей связи для экстренного предупреждения о факторах уязвимости, угрозах и инцидентах в ИКТ-среде;

b) повышение степени информированности заинтересованных сторон, с тем чтобы они глубже понимали характер и масштабы своих важнейших информационных инфраструктур и ту роль, которую каждая из них должна играть в защите этих инфраструктур;

49 Forewords by the Secretary-General. A/70/174

50 For example, the Convention (No.174) concerning the Prevention of Major Industrial Accidents (Geneva 1993) Convention on the Physical Protection of Nuclear Material (Vienna 1979); Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Montreal 1971); Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (Rome 1988).

51 A/58/199/. Приложение.

c) анализ инфраструктур и выявление факторов, обусловливающих их взаимозависимость, для усиления защиты таких инфраструктур;

d) содействие развитию партнерских отношений заинтересованными сторонами, представляющими как государственный, так и частный секторы, для обмена информацией о важнейших инфраструктурах и ее анализа в целях предотвращения нанесения ущерба таким инфраструктурам или попыток нарушения их защиты, расследования случаев нанесения ущерба объектам защищаемой инфраструктуры;

e) создание и обеспечение функционирования систем коммуникации в кризисной ситуации и проверка их функционирования для обеспечения их надежной и стабильной работы в чрезвычайных ситуациях;

f) обеспечение того, чтобы процедуры предоставления доступа к данным учитывали необходимость защиты важнейших информационных инфраструктур;

g) содействие отслеживанию попыток взлома защиты важнейших информационных инфраструктур и, в надлежащих случаях, предоставление информации о результатах такого отслеживания другим государствам;

h) организация профессиональной подготовки и проведение тренировок для укрепления потенциала реагирования и апробирования планов обеспечения непрерывной работы и резервных планов на случай попыток взлома защиты информационных инфраструктур, а также побуждение заинтересованных сторон к участию в аналогичных мероприятиях;

i) наличие адекватных материальных и процессуальных законов и квалифицированного персонала для того, чтобы государства могли расследовать попытки нарушения защиты важнейших информационных инфраструктур и привлекать к ответственности причастных к этим попыткам лиц, а также в надлежащем порядке координировать такие расследования с другими государствами;

j) участие, когда это уместно, в международном сотрудничестве для обеспечения защищенности важнейших информационных инфраструктур, в том числе путем создания и координации работы систем срочного предупреждения, для обмена информацией о факторах уязвимости, угрозах и инцидентах и анализа такой информации, а также для координации расследований попыток взлома защиты таких инфраструктур в соответствии с национальным законодательством;

k) содействие национальным и международным научным исследованиям и опытно-конструкторским разработкам и поощрение применения технологий обеспечения защиты, отвечающих международным стандартам.

66. Важным направлением международного сотрудничества в области применения комментируемой рекомендации может стать участие государств в совершенствовании системы международных стандартов технического регулирования[52], которые направлены на обеспечение соответствующего уровня защиты и организации управления информационными инфраструктурами, а также на поддержание функционирования критической инфраструктуры.

67. В целях повышения доверия и расширения сотрудничества ГПЭ ООН рекомендует государствам рассмотреть следующие добровольные меры укрепления доверия[53]:

a) определение надлежащих контактных центров на политическом и техническом уровнях для рассмотрения серьезных инцидентов в сфере ИКТ и создание перечня таких центров;

b) создание и поддержка механизмов и процессов для проведения двусторонних, региональных, субрегиональных и многосторонних консультаций, сообразно обстоятель-

52 ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cyber security; ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems – Requirements; ISO 22301 Societal security -- Business continuity management systems --- Requirements; ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security; ISO/IEC 27035 Information technology -- Security techniques -- Information security incident management; ISO/IEC 27005 Information technology -- Security techniques -- Information security risk management; FIPS 140-1: Security Requirements for Cryptographic Modules; FIPS 186-3: Digital Signature Standard.
53 A/70/174 para16

ствам, в целях укрепления доверия между государствами и снижения риска ошибочного восприятия, эскалации и конфликта, которые могут быть вызваны инцидентами в сфере ИКТ;

c) содействие на добровольной основе повышению транспарентности на двустороннем, субрегиональном, региональном и многостороннем уровнях, сообразно обстоятельствам, в целях повышения доверия и определения направлений дальнейших исследований. Это может включать добровольное распространение национальных мнений и информации о различных аспектах национальных и транснациональных угроз ИКТ и в сфере использования ИКТ; факторах уязвимости и установленных пагубных скрытых функций в продуктах ИКТ; передовых методах обеспечения безопасности ИКТ; мерах укрепления доверия, разработанных в рамках региональных и многосторонних форумов; национальных организациях, имеющих отношение к безопасности ИКТ;

d) добровольное представление государствами информации об их национальных мнениях в отношении категорий инфраструктуры, которые они считают критически важными, а также о национальных усилиях по ее защите, включая информацию о национальных законах и стратегиях обеспечения безопасности данных и инфраструктуры, зависящей от ИКТ. Государства должны стремиться укреплять трансграничное сотрудничество в устранении транснациональных факторов уязвимости критически важной инфраструктуры ИКТ, которые выходят за пределы национальных границ. Такие меры могут включать:

i) создание базы данных по национальному законодательству и стратегиям обеспечения безопасности данных и инфраструктуры, зависящей от ИКТ, а также публикация материалов, считающихся важными для целей распространения информации об этих национальных законах и стратегиях;

ii) создание механизмов и процессов для проведения двусторонних, субрегиональных, региональных и многосторонних консультаций по вопросам защиты критически важной инфраструктуры, зависящей от ИКТ;

iii) создание двусторонних, субрегиональных, региональных и многосторонних основ технических, правовых и дипломатических механизмов для рассмотрения запросов, связанных с ИКТ;

iv) принятие добровольных национальных договоренностей о классификации инцидентов в сфере ИКТ с точки зрения масштабов и серьезности инцидента для целей содействия обмену информацией об инцидентах[54].

Проблемы имплементации

68. В рамках специализированных режимов международного права сотрудничество в области защиты критической инфраструктуры также координируется посредством таких специализированных организаций как МАГАТЭ, Международная морская организация и ИКАО. В то же время существующие международные договоры, затрагивающие вопросы применения стандартов и требований к защите определенных объектов, секторов, функций и услуг, не охватывают всю критическую инфраструктуру.

69. В то же время, резолюции о создании глобальной культуры кибербезопасности не предусматривают универсальный механизм международного сотрудничества и координации. Эти резолюции[55] содержат направления деятельности, ориентированные на национальный уровень, без увязки со специальным международным механизмом или платформой сотрудничества.

70. Недостаточная защита критической инфраструктуры или национальной информационной инфраструктуры может привести к международному спору. Разрешение спора с использованием предложенных в Уставе ООН способов может оказаться затруднительным ввиду следующего:

54 UN A/70/174

55 Резолюция ГА ООН по глобальной культуре кибербезопасности. 64/211 (2010).

a) отсутствие согласованных на международном уровне признаков критической инфраструктуры;

b) отсутствие согласованных на международном уровне критериев безопасности критической инфраструктуры;

c) отсутствие способов получения доказательств возникновения инцидентов в ИКТ-среде, связанной с критической инфраструктурой и национальной информационной инфраструктурой;

d) отсутствие согласованных на международном уровне процедур проведения расследования инцидентов.

71. Для ликвидации пробелов в правовом регулировании отношений в ИКТ-среде добровольные усилия государств могут быть направлены на: a) установление или закрепление состава национальной информационной инфраструктуры (например, перечни объектов, входящих в национальную инфраструктуру); б) воздержание от нанесения вреда информационным инфраструктурам других государств; в) установление адекватной защиты их собственных информационных инфраструктур; г) определение порядка проведения совместных расследований по признакам инцидентов в национальной ИКТ-среде, связанным с нарушением стабильности функционирования этой среды. Такие рекомендации могли бы стать частью универсальной, региональной или многосторонней системы обеспечения надлежащего уровня защищенности критической информационной инфраструктуры от угроз в сфере ИКТ.

V.2. Параграф 13 h) доклада ГПЭ ООН 2015 г.

Предмет, объект и цель регулирования

72. Согласно параграфу 13 (h) Доклада, «государства должны удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ. Государства должны также удовлетворять соответствующие просьбы о смягчении последствий злонамеренных действий в сфере ИКТ, направленных против критически важной инфраструктуры других государств, если такие действия проистекают с их территории, принимая во внимание должным образом концепцию суверенитета».

73. Применение данной рекомендации можно рассматривать как способ применения в ИКТ-среде принципов дружеских отношений и сотрудничества среди государств и вклад в достижение целей ООН.

74. Государства неоднократно заявляли о необходимости совместных действий, нацеленных на устранение угроз злонамеренного использования ИКТ[56]. Такие действия могут включать развитие взаимопонимания относительно применения соответствующих норм международного права как основы имплементации рекомендаций по ответственному поведению государств в ИКТ-среде. Это будет способствовать укреплению международного мира, стабильности и безопасности. Кроме того, государства могли бы активизировать сотрудничество в борьбе с использованием ИКТ в преступных и террористических целях, должным образом согласовывать и развивать практическое сотрудничество между соответствующими законодательными и правоохранительными органами[57].

75. Злонамеренное использование ИКТ может нанести серьезный ущерб экономике в целом, а также национальной и международной безопасности. Такие действия могут быть направлены против физических и юридических лиц, национальной инфраструктуры и государств. Они могут способствовать возникновению существенных рисков для общественной безопасности, безопасности государств и стабильности в международном сообществе в целом, объединенном глобальной информационной инфраструктурой.

*56 A/68/98**
57 A/65/201, para.12.

76. «На протяжении прошедшего десятилетия государства-члены ООН неоднократно подтверждали необходимость развития международного сотрудничества в области противодействия угрозами безопасности ИКТ-среды, злонамеренного применения ИКТ в преступных целях, а также необходимость создания глобальной культуры кибербезопасности и поощрения других важных мер, которые могут уменьшить риск нарушения устойчивости функционирования и безопасности использования информационной инфраструктуры» [58].

77. Предметом рекомендации являются международные отношения в области взаимной помощи.

78. Объектом рекомендации являются добровольные обязательства государств по следующим вопросам: a) помощь другим государствам в связи с злонамеренными действиями криминального, террористического и враждебного характера против их критической инфраструктуры в области ИКТ; b) содействие уменьшению тяжести последствий злонамеренных действий в отношении национального сегмента ИКТ-среды, являющегося критической информационной инфраструктурой.

79. Предполагается, что национальная инфраструктура государства, к которому обращаются за помощью, использовалась для совершения соответствующих злонамеренных действий или данное государство обладает соответствующими возможностями для оказания такой помощи. Предполагается, что помощь могла бы уменьшить серьезность последствий от злонамеренных действий в области использования ИКТ, повлиявших на функционирование критической инфраструктуры.

80. Цель рекомендации состоит в создании правовых условий для укрепления устойчивости функционирования критической инфраструктуры посредством снижения негативного влияния злонамеренных действий в сфере ИКТ на критическую инфраструктуру и, как следствие, — для укрепления международного мира и безопасности.

Возможные направления обсуждения имплементации рекомендации

81. Исследуемая норма регулирует новую группу международных отношений по поводу добровольного оказания помощи другим государствам в чрезвычайной ситуации в ИКТ-среде.

82. Потенциальная применимость международного права к рассматриваемым отношениям следует, *inter alia*, среди прочего, из положений Устава ООН, Декларации принципов международного права[59], Соглашения о помощи[60], Соглашения по трансграничным усилиям в случае несчастных случаев на производстве[61], Соглашения о предоставлении телекоммуникационных ресурсов[62]. В соответствующих обстоятельствах помощь может также быть оказана на основе Конвенции ООН против Межнациональной Организованной преступности[63].

83. В соответствии с Резолюцией 57/150 Генеральной Ассамблеи ООН от 16 декабря 2002 г. «каждое государство, прежде всего, ответственно за обеспечение помощи жертвам стихийных бедствий, происходящих на его территории, и поэтому государство, затронутое бедствием, должно играть главную роль «в инициировании, организации, координировании и обеспечении гуманитарной помощи на его территории».

84. В настоящее время государства не имеют специального обязывающего между-

58 Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. 30 июля 2010 , A/65/201

59 Resolution 2625 of the UN General Assembly on October 24, 1970

60 Convention on Assistance in the Event of a Nuclear or Radiological Emergency. General Conference of the International Atomic Energy Agency. September 26, 1986.

61 Convention on the Transboundary Effects of Industrial Accidents. Helsinki, 17 March 1992, E/ECE/1268.

62 The Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations. Tampere. June 18, 1998.

63 United Nations Convention against Transnational Organized Crime (Palermo 2000).

народного обязательства об оказании помощи в чрезвычайных ситуациях, являющихся результатом злонамеренных действий с использованием ИКТ против национального сегмента критической информационной инфраструктуры.

Ремарка. Некоторые эксперты подчеркнули, что механизмы многосторонней взаимопомощи в уголовном праве и других правовых вопросах представляют собой международную основу, которая является обязательной и может служить основанием для оказания помощи.

85. Кроме того, отсутствуют широко известные примеры применения норм «мягкого права» для регулирования международных отношений в области обеспечения помощи и смягчения последствий злонамеренного использования ИКТ против национальных сегментов критической информационной инфраструктуры.

Ремарка. Некоторые эксперты придерживались противоположного взгляда. Известно много примеров успешного сотрудничества и помощи между государствами в случае кибератак, например, между службами первой медицинской помощи, правоохранительными органами, а также между дипломатами и политическими лицами, принимающими решение.

86. Основная проблема применения рассматриваемой рекомендации заключается в трудности идентификации государства, с территории которого осуществлялись злонамеренные действия против национального сегмента критической информационной инфраструктуры или национальной критической инфраструктуры. Это усложняет применение юридических процедур по решению международных споров или недоразумений.

Ремарка. Некоторые эксперты придерживались мнения, что для всех, и особенно для тех, кому ошибочно приписывается ответственность, должно быть интересно решить вопрос совместно, а не отрицать свое участие или не давать никаких комментариев. Эти эксперты пришли к заключению, что основные проблемы применения рассматриваемой рекомендации касаются потенциально деликатного характера инцидента и различий в возможностях государств по оказанию обоснованной помощи без рисков нанесения ущерба их собственной безопасности.

V.3. Параграф 13 k) доклада ГПЭ ООН 2015 г.

Предмет, объект и цель регулирования

87. Согласно рекомендации 13 (k), «государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным инцидентам (также именуемым группами готовности к компьютерным инцидентам или группам готовности к инцидентам в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности».

88. Применение изучаемой рекомендации может базироваться на следующих принципах:

a) «государственный суверенитет и международные нормы, и принципы, вытекающие из принципа государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием ИКТ, а также на юрисдикцию государств над ИКТ-инфраструктурой на их территории».[64]

b) «ни одно государство или группа государств не имеет права вмешиваться прямо или косвенно по какой бы то ни было причине во

64 A/68/98*, n.20

внутренние и внешние дела любого другого государства»;

c) «ни одно государство не может ни применять, ни поощрять применение экономических, политических мер или мер любого иного характера с целью добиться подчинения себе другого государства в осуществлении им своих суверенных прав и получения от этого каких бы то ни было преимуществ» [65].

89. Предметом рекомендации являются международные отношения в области обеспечения безопасности выполнения задач, возложенных на центры реагирования на компьютерные инциденты (далее — ЦРКИ).

90. Объектом рекомендации являются международные отношения по поводу предотвращения, обнаружения, реакции на инцидент в ИКТ-среде и восстановления после инцидента. В этих отношениях уполномоченные ЦРКИ играют активную и центральную роль. Предполагается, что ЦРКИ обладают полномочиями и обязанностями в области реагирования на инцидент, связанный с национальной критической информационной инфраструктурой. Информационные системы[66] ЦРКИ поддерживают выполнение возложенных на них задач.

91. Целью рекомендации является создание условий для добровольного принятия государствами международных обязательств, связанных с запретом осуществления и поддержания деятельности в сфере ИКТ, которая могла бы нанести ущерб информационным системам уполномоченных ЦРКИ, а также доверию между ними. Эта рекомендация направлена на предотвращение использования уполномоченных ЦРКИ для выполнения злонамеренных международных действий. Регулирование осуществляется посредством установления запрета осуществления и сознательной поддержки действий управляемых государством структур, направленных на причинение ущерба информационным системам ЦРКИ как одному из элементов, обеспечивающих безопасность национального сегмента критической информационной инфраструктуры.

Возможные направления обсуждения имплементации рекомендации

92. Запрещение преднамеренной деятельности или ее поддержки, причиняющей ущерб ЦРКИ, по существу, означает предоставление этим объектам специальных или международных гарантий безопасности. Это может быть достигнуто путем установления специального политического или правового международного режима для ЦРКИ.

93. В настоящее время нарушение запрета, предусматриваемого рассматриваемой рекомендацией, может интерпретироваться как нарушение принципа международного права, предусматривающего невмешательство в дела, входящие во внутреннюю компетенцию. Согласно этому обязательному принципу, государства обязаны не вмешиваться в вопросы, находящиеся в пределах внутренней юрисдикции любого другого государства, включая нарушение правомерно установленного государством правового режима безопасности информационных систем ЦРКИ.

94. Добровольное соблюдение предлагаемого запрета — одно из средств создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Запрет на использование ЦРКИ для злонамеренных международных действий

65 Принцип, касающийся обязанности в соответствии с Уставом не вмешиваться в дела, входящие во внутреннюю компетенцию любого другого государства. Декларация принципов международного права. 1970.

66 В Федеральном законе «Об информации, информационных технологиях и о защите информации» (№149-ФЗ) понятие «информационная система» раскрывается как «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств».

US Law uses the term "information system" as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information" (44 USCS § 3502, https://definitions.uslegal.com/i/information-system/);

The Encyclopedia Britannica uses the term "Information system" as "an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products", (/www.britannica.com/topic/information-system).

может быть достигнут посредством принятия соответствующих международных обязательств, а также применения нормативных правовых актов национального законодательства.

95. К инцидентам относятся события, которые прерывают процедуру обработки информации, предусмотренную эксплуатационной документацией, и которые имеют существенные негативные последствия для качества функционирования национальной инфраструктуры. В частности, такие инциденты могут проявляться в форме внедрения вредоносного программного обеспечения, атак типа «отказ в обслуживании», несанкционированного доступа к информации и другим незаконным действиям.

96. Уполномоченные ЦРКИ могут управляться как правительственными, так и неправительственными организациями на коммерческой основе. Их компетенция устанавливается национальным законодательством. Например, ЦРКИ может осуществлять:

a) подтверждение или опровержение самого факта инцидента;

b) сбор достоверной информации об инциденте; контроль правильности обнаружения и сбора установленных законом и политикой безопасности фактов, включая факты нарушения гражданских прав;

c) минимизация воздействия на деловые и сетевые операции; содействие подаче гражданских исков и инициирование возбуждения уголовных дел против нарушителей;

d) создание детального отчета и подготовка полезных рекомендаций для будущих реакций на инциденты, и т.д.

97. В настоящее время отсутствуют примеры применения государствами норм «мягкого права» для регулирования международных отношений в области обеспечения защиты информационных систем ЦРКИ.

Ремарка. Данная точка зрения не была поддержана некоторыми экспертами, которые отметили, что широкое и доверительное сотрудничество, между ЦРКИ предлагает определенные гарантии не только взаимодействия по поводам инцидентов и кризисов, но также и неприкосновенность ЦРКИ. Более того, они сослались на Устав ООН, который запрещает использование силы и вмешательство и определяет нормативные правовые и обычные правила поведения государств как в ИКТ-среде, так и киберпространстве.

98. Применение этой рекомендации усложнено ввиду нежелания государств использовать правовые средства разрешения соответствующих международных споров или недоразумений. В частности, российские авторы считают проблематичными: обвинение против государств в связи со злонамеренным использованием ИКТ против информационных систем национального сегмента информационной инфраструктуры, также как в связи с злонамеренным использованием ЦРКИ для нанесения вреда национальному сегменту информационной инфраструктуры; приписывание ответственности государствам в связи с обвинением их в действиях или преднамеренной поддержке действий, наносящих ущерб информационным системам ЦКРИ; обвинение государства в злонамеренных международных действиях. В современных условиях такие обвинения, как правило, не подкрепляются объективными фактами, что создает риск приписывания международной правовой ответственности государствам на основе исключительно политических предпочтений.

Ремарка. Другие эксперты подчеркнули, что выбор применения закона мирного урегулирования международных споров всегда открыт для государств. Проблема отсутствия правовых инструментов разрешения споров является важной для стратегических соперников, но не обязательно отражает взгляды и опыт всех государств. Эксперты согласились с тем, что приписывание ответственности остается проблемным вопросом, но в основном из-за недостаточных национальных потенциалов.

99. Выделенные проблемы способствуют увеличению риска возникновения международного спора, у которого отсутствует перспектива решения правовыми средствами.

100. Некоторые эксперты полагают, что для достижения цели рекомендации необходимо: a) определение международной организации, уполномоченной проводить расследования международных инцидентов в ИКТ-среде, в том числе с использованием ЦКРИ; b) развитие рекомендаций для проведения таких расследований с участием представителей заинтересованных государств; c) принятие рекомендаций по признакам и особенностям злонамеренных действий. Данные предположения не мешают продолжению диалога по всему спектру возможных направлений дальнейшего сотрудничества.

Ремарка. Другие эксперты рекомендуют диалог о способах реализации рассматриваемой рекомендации и обмена национальными представлениями по данному вопросу. Они также скептически относятся к необходимости организации международных расследований и приписывания международной правовой ответственности.

VI. Выводы и рекомендации

101. Государства могут и должны применять международное право к международным отношениям в ИКТ-среде. Текущее международное правовое регулирование использования ИКТ государствами может порождать международные споры, способные привести к нарушению международного мира и безопасности. Для повышения действенности применения международного права к отношениям в ИКТ-среде Генеральная Ассамблея ООН призвала государства исследовать возможные направления прогрессивного развития международного права.

102. На существующем этапе развития международных отношений принятие норм, правил и принципов ответственного поведения государств в ИКТ-среде представляется более многообещающей перспективой, чем другие направления исследования государствами международного права.

103. Механизм добровольных и необязательных норм, правил и принципов ответственного поведения государств в ИКТ-среде предназначен для содействия формированию более совершенных международных норм посредством постоянной и однородной государственной практики. Процесс обсуждения рекомендаций по ответственному поведению государств в использовании ИКТ позволяет также обмениваться информацией по поводу общих ожиданий, лучших практик и опыте.

104. Текущее состояние международных отношений позволяет научному сообществу и политикам изучать возможности практического применения норм, правил и принципов ответственного поведения государств в ИКТ-среде. «Мягкое право», т.е. право, нормы которого не влекут правовые последствия в случае их нарушения, создает условия для постепенного применения международного права, для достижения обязательных и универсальных стандартов поведения.

105. Практическое применение рекомендаций по ответственному поведению государств в ИКТ-среде как средства регулирования международных отношений может явиться важным этапом укрепления безопасности использования государствами ИКТ.

106. Некоторые эксперты пришли к заключению, что добровольное применение рекомендаций по ответственному поведению государств в ИКТ-среде может быть реализовано в форме двусторонних, многосторонних, региональных соглашений и соглашений универсального характера. Другие эксперты отметили, что это может быть сделано без правовых обязательств, т.е. на основе добровольной практики. В любом случае имплементация должна быть дополнена необходимым национальным нормативным правовым регулированием.

Комментарий экспертов Института киберполитики, Фонда «ИКТ для мира», поддержанный экспертами Института Восток-Запад

Это не часто случается, когда западные ученые получают возможность работать с их российскими коллегами над проблемами международной информационной безопасности или кибербезопасности. Отсутствие контактов создает трудности в поиске путей продвижения вперед в условиях политических различий и конкурирующих мировоззрений.

Мы сочли наше сотрудничество с российскими коллегами чрезвычайно информативным и полезным, поскольку оно помогло нам понять российские позиции и представления по некоторым проблемам. Мы вошли в этот проект по приглашению Международного информационного Консорциума Исследования безопасности и Московского государственного университета для того, чтобы лучше понять, как наши коллеги подходят к проблеме применения норм, правил и принципов ответственного государственного поведения, представленных в Докладе ГПЭ ООН 2015 г.

Завершая этот проект, мы можем прийти к заключению, что существуют не только политические, но также и фундаментальные методические различия в том, как западные и российские ученые подходят к необязательным нормам и международному праву. Существующие различия делают почти невозможным для западных коллег признание и оценку предложений, вносимых российскими коллегами по вопросу применения рекомендаций ГПЭ ООН и сделать их общепринятыми. Независимо от того, будет ли найденное решение базироваться на этих различиях или нет, мы считаем необходимым выдвигать на первый план эти различия, чтобы облегчить поиск консенсуса и путей к международному обсуждению международной безопасности кибербезопасности/информационной безопасности.

Эксперты в этой очень небольшой группе остались разделенными в трех фундаментальных вопросах:

1) соответствие существующего международного права и текущей практики государств поддержанию рекомендуемого поведения государств. Российские коллеги намного более пессимистичны о возможности применения существующих правил и стандартов международного права к проблемам кибербезопасности без прогрессивного развития этого права. Основанный на нашем опыте и экспертных знаниях, мы считаем возможным применить правила и стандарты существующего международного права такие, как запрет на вмешательство во внутренние дела или обязательство мирного урегулирования международных споров, к проблемам международной кибербезопасности. Это действительно требует диалога между государствами относительно путей лучшей интерпретации и применения этих правил и стандартов.

2) природа рекомендаций по нормам, правилам и принципам ответственного поведения государств, изложенных в Докладе ГПЭ ООН 2015. В российской концепции эти нормы, правила и принципы будут осуществлены только после того, как они приобретут юридически обязательный статус, или государственную практику или переговоров по соглашению. С нашей точки зрения ООН рекомендации ГПЭ могут быть осуществлены частично на основе существующего международного права и частично посредством национального законодательства и политики, которая, как российские коллеги указывают, реализуется на основе суверенитета.

3) соответствие вопроса об атрибуции трем исследованным рекомендациям ГПЭ ООН. Различия по вопросу об атрибуции, особенно по отношению к стратегическим соперникам и, между этими государствами, породили опасения относительно возможности удовлетворительного внедрения международного права. Для большинства государств, однако, приписывание остается вопросом развития способностей и возможностей. Поэтому рано делать заключение о том, является ли проблема атрибуции действительно важной проблемой международного права для международного сообщества, или она может

быть решена посредством практики улучшения и увеличение национальной устойчивости и способности.

Эти вопросы являются также ключевыми вопросами на политических переговорах, как глобального, так и двустороннего характера. Поэтому, мы приходим к заключению, что успешное и глобальное внедрение рекомендуемых норм маловероятно до тех пор, пока страны придут к соглашению относительно их предпосылок и предположений.

Самое главное, учитывая эти основополагающие различия, обмен мнениями, совместное научное исследование и политический диалог должны продолжиться. Это взаимодействие должно так же принять междисциплинарный характер и вовлечь широкое сообщество ученых и экспертов.

Для заметок

Для заметок