

**НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ МЕЖДУНАРОДНОЙ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**NATIONAL ASSOCIATION FOR INTERNATIONAL
INFORMATION SECURITY**



**ПРИМЕНЕНИЕ НОРМ
ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ
ГОСУДАРСТВ В ИКТ-СРЕДЕ
И МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО**

(РЕФЕРАТ ПО РЕЗУЛЬТАТАМ ИССЛЕДОВАНИЯ)

**APPLICATION OF THE NORMS
OF RESPONSIBLE BEHAVIOR OF STATES
IN THE ICT ENVIRONMENT
AND INTERNATIONAL COOPERATION**

(ABSTRACT ON THE RESULTS OF THE STUDY)

**Москва / Moscow
2022**

АВТОРСКИЙ КОЛЛЕКТИВ

1. **Стрельцов Анатолий Александрович** – д.ю.н, д.т.н., проф.,
руководитель работы
2. **Капустин Анатолий Яковлевич** – д.ю.н., проф.
3. **Смирнов Александр Александрович** – к.ю.н.
4. **Полякова Татьяна Анатольевна** – д.ю.н., проф.
5. **Касёнова Мадина Балташевна** – д.ю.н., проф.
6. **Русинова Вера Николаевна** – д.ю.н., проф.
7. **Шинкарецкая Галина Георгиевна** – д.ю.н., проф.
8. **Жарова Анна Константиновна** – д.ю.н., доцент
9. **Пилюгин Павел Львович** – к.т.н., доцент
10. **Калицев Александр Евгеньевич**
11. **Горжалцан Владимир Ахиллович**
12. **Герасимов Андрей Васильевич**
13. **Марков Алексей Сергеевич** - д.т.н., проф.
14. **Милославская Наталья Георгиевна** – д.т.н., проф.
15. **Мирошников Борис Николаевич** – к.ю.н.
16. **Панин Александр Вячеславович**
17. **Коротков Сергей Васильевич** – к.в.н.
18. **Бойко Константин Сергеевич**
19. **Волкова Светлана Геннадьевна**

ОГЛАВЛЕНИЕ

Введение.....	6
1. Среда информационно-коммуникационных технологий как пространство сотрудничества	8
2. Проблемы применения норм ответственного поведения государств в ИКТ-среде.....	10
3. Предложения по решению проблем применения норм ответственного поведения государств в ИКТ-среде	12
4. Основные направления международного сотрудничества в целях применения норм ответственного поведения государств в ИКТ-среде.....	14
Заключение	18

TABLE OF CONTENTS

Introduction.....	22
1. The environment of information and communication technologies as a space for cooperation	24
2. Problems of application of norms of responsible behavior of States in the ICT environment	25
3. Proposals for solving the problems of applying the norms of responsible behavior of States in the ICT environment	27
4. Main directions of international cooperation in order to apply the norms of responsible behavior of States in the ICT environment.....	29
Conclusion	33

ПРЕДИСЛОВИЕ

Цифровые технологии в XXI веке стали неотъемлемым атрибутом практически всех сторон жизни национальных обществ и международного сотрудничества. Безопасное использование глобальной среды информационных и коммуникационных технологий, а также устойчивое функционирование ее национальных сегментов в современном мире являются одним из условий поддержания международного мира и безопасности.

Вместе с тем продолжающаяся «цифровая трансформация» жизни человека и человечества порождает и новые риски. Глобальное информационное пространство все чаще превращается в поле информационного противоборства политических сил общества, нечестной конкуренции коммерческих организаций, жестких конфликтных отношений между государствами. Глобальную среду информационных и коммуникационных технологий активно используют международные террористы и организованная преступность.

В этой связи представляется исключительно своевременной поддержанная Ассоциацией инициатива российских экспертов по изучению проблем применения норм ответственного поведения государств в ИКТ-среде. Результаты проведенного исследования представлены в настоящем реферативном материале и предложены для обсуждения на третьей субстантивной сессии Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021–2025.

Уверен, что обсуждение результатов исследования российских экспертов будут способствовать формированию нового уровня понимания проблемы правового обеспечения международной информационной безопасности.

Президент Национальной Ассоциации международной информационной безопасности, советник Секретаря Совета Безопасности Российской Федерации, член-корреспондент Академии криптографии Российской Федерации

Владислав Шерстюк

ВВЕДЕНИЕ

Активное развитие информационных и коммуникационных технологий (ИКТ) и рынка продуктов ИКТ, глобальной информационной инфраструктуры, расширение использования этих технических ресурсов для оказания коммуникационных и информационных услуг, а также увеличение количества пользователей этими услугами и продуктами ИКТ в различных сферах деятельности, являются важными факторами изменения жизни общества. Эти процессы, с одной стороны, содействуют возникновению новой среды жизни человека – среды информационно-коммуникационных технологий (далее – ИКТ-среда), а с другой – создают условия для формирования глобального информационного общества.

Предполагается, что в информационном обществе у каждого будет возможность «создавать информацию и знания, иметь к ним доступ, пользоваться и обмениваться ими», а также что у отдельных лиц, общин и народов будет «возможность в полной мере реализовать свой потенциал, содействуя своему устойчивому развитию и повышая качество своей жизни»¹.

Уровень доступности ИКТ, готовность граждан, организаций и государства к использованию этих технологий в практической деятельности становятся индикаторами изменения социокультурных условий жизни людей и становятся символами нового информационного «измерения» этой жизни².

В информационном обществе безопасность использования ИКТ-среды становится одним из важнейших факторов устойчивого развития³. В то время как злонамеренное использование ИКТ недобросовестными государствами и другими субъектами международной жизни создает существенные риски для «международной безопасности и стабильности, экономического и социального развития, для безопасности благополучия отдельных лиц»⁴.

¹ Декларация принципов. Построение информационного общества – глобальная задача в новом тысячелетии. Всемирная встреча на высшем уровне по вопросам информационного общества. 12 декабря 2003 г. п.1. WSIS-03/GENEVA/DOC/4-R

² Информационное общество в Российской Федерации. Статистический сборник. НИУ ВШЭ. М., 2017.

³ Декларация принципов. Построение информационного общества – глобальная задача в новом тысячелетии. Всемирная встреча на высшем уровне по вопросам информационного общества. 12 декабря 2003 г. п.9. <https://www.itu.int/net/wsis/index-ru.html>.

⁴ Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве ИКТ-среды в контексте международной безопасности (Доклад A/76/135, 2021 г.). п.6.

Как показывают результаты работы Генеральной Ассамблеи ООН государства – члены международного сообщества все более пристальное внимание обращают на вопросы обеспечения безопасности использования ИКТ, устойчивости функционирования глобальной ИКТ-среды.

Обеспечение безопасности использования глобальной ИКТ-среды на основе применения норм и принципов международного права сталкивается с рядом объективных трудностей. Этим обусловлено предложение ряда государств – членов Шанхайской организации сотрудничества рассмотреть на Генеральной Ассамблее ООН правила поведения в области обеспечения международной информационной безопасности⁵. Правила, предложенные государствами Шанхайской организации сотрудничества, создали методологическую основу для подготовки Группами правительственных экспертов (2015 г., 2021 г.) норм, правил и принципов (далее – норм) ответственного поведения государств в ИКТ-среде⁶, а также материалов Рабочей группы открытого состава ООН (2021г.)⁷.

По мнению международного сообщества применение норм ответственного поведения государств в ИКТ-среде параллельно с применением принципов и норм международного права может способствовать укреплению международного мира и безопасности.

В целях содействия обсуждению на площадке Рабочей группы открытого состава ООН вопроса о применении норм ответственного поведения государств в ИКТ-среде Национальной Ассоциацией международной информационной безопасности подготовлен настоящий реферативный материал. Материал отражает результаты проводимого Национальной Ассоциацией экспертного исследования проблем практического применения этих норм в деятельности государств.

По мнению российских экспертов, успешность применения норм ответственного поведения в качестве средства регулирования международных

⁵ Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 года на имя Генерального секретаря ООН (A/66/359), Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря ООН (A/69/723)

⁶ Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/70/174), Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности (A/76/135)

⁷ Заключительный основной доклад Рабочей группы открытого состава ООН по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности от 10 марта 2021 г. A/AC.290/2021/CRP.2

отношений в ИКТ-среде будет зависеть от решения ряда сложных проблем, обусловленных, прежде всего, особыми свойствами этого нового пространства международного сотрудничества.

1. СРЕДА ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ КАК ПРОСТРАНСТВО СОТРУДНИЧЕСТВА

1.1. ИКТ-среда образуется совокупностью информационной инфраструктуры (информации, расположенной на электронно-вычислительных устройствах; цифровых ИКТ обработки информации; коммуникационных сетей и сетей связи) и пользователей, использующих эту инфраструктуру для участия в разнообразных общественных отношениях. Формирование национального сегмента ИКТ-среды является важным фактором развития российского общества и государства.

Информационно-коммуникационная инфраструктура является основой национального сегмента ИКТ-среды и одновременно – одной из ключевых составляющих инфраструктуры Российской Федерации.

Безопасность использования национального сегмента ИКТ-среды и устойчивость функционирования национальной информационной инфраструктуры (информационная безопасность) оказывают существенное влияние на национальную безопасность Российской Федерации.

1.2. Национальный сегмент ИКТ-среды является составной частью глобальной ИКТ-среды, техническую основу которой составляют глобальные сети связи и глобальная информационно-коммуникационная сеть Интернет.

Злонамеренная и вредоносная деятельность некоторых государств и иных субъектов, осуществляемая в военных, террористических и преступных целях на национальном, региональном и глобальном уровнях, становится все более серьезной угрозой международному миру и безопасности.

Особую озабоченность вызывает злонамеренная и вредоносная деятельность в сфере использования ИКТ, которая затрагивает критически важную инфраструктуру. Безопасность и устойчивость функционирования критически важной инфраструктуры в современном обществе зависит от безопасности использования ИКТ. Критическая важность этой инфраструктуры обусловлена ее использованием для предоставления основных услуг населению, для обеспечения общей доступности и целостности сети Интер-

нет, а также для деятельности организаций гражданского общества в экономической, социальной, политической и культурной сферах, для эффективной деятельности органов управления государством.

В обозримой перспективе значение безопасности использования ИКТ и устойчивости функционирования информационной инфраструктуры как факторов обеспечения национальной и международной безопасности будет увеличиваться.

1.3. ИКТ-среда как пространство международного сотрудничества обладает свойствами, принципиальным образом отличающими ее от свойства традиционных пространств реализации территориального суверенитета государств и международного сотрудничества (суша, морское, воздушное, космическое пространство и недра).

К числу отличительных свойств ИКТ-среды как пространства сотрудничества относятся: особый характер общественных отношений, реализуемых с использованием этого пространства (информационные отношения); особые свойства информации как объекта обработки с использованием ИКТ (виртуальность); особый характер способов поддержания функционирования ИКТ-среды как пространства осуществления информационной деятельности человека (партнерство государства и бизнеса); особый правовой статус человека как субъекта информационной деятельности, в том числе и в ИКТ-среде (свобода информационной деятельности).

1.4. Нормы ответственного поведения государств в ИКТ-среде могут стать средством правового регулирования международных отношений при условии их закрепления в международном соглашении. В настоящее время эти нормы представляют собой рекомендательные, юридически необязательные правила поведения государств, перечисленные в докладах Групп правительственных экспертов⁸ и рекомендованные государствам для рассмотрения резолюциями Генеральной Ассамблеи ООН⁹.

Эти правила поведения государств вытекают из общих принципов общественной морали и дополняют нормы международного и национального права, а также нормы «мягкого права», закрепленные в международных политических договоренностях.

Нормы ответственного поведения государств после их закрепления в международном соглашении могут учитываться при толковании действу-

⁸ A/70/235, A/76/135

⁹ A/70/134, A/75/240

ющих международно-правовых норм, содействовать возникновению новых международных обычаев и служить ориентиром при заключении международных договоров.

1.5. Применение норм ответственного поведения государств в ИКТ-среде является одной из форм реализации международных обязательств государств, осуществляемой с учетом норм и принципов международного права и национального законодательства.

2. ПРОБЛЕМЫ ПРИМЕНЕНИЯ НОРМ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИКТ-СРЕДЕ

2.1. Применение норм ответственного поведения государств в ИКТ-среде для регулирования международных отношений и общественных отношений, относящихся к национальной юрисдикции, сталкивается с рядом фундаментальных проблем.

2.2. Во-первых, нормы ответственного поведения государств в ИКТ-среде не вытекают непосредственно из существующих норм международного права, т.е. не являются положениями *lex lata* международного публичного права. Эти нормы направлены на уточнение толкования существующих норм международного права применительно к отношениям в ИКТ-среде, а также на расширение состава международной нормативной системы, регулирующей деятельность в области использования ИКТ.

Вследствие этого для применения норм ответственного поведения государств в ИКТ-среде необходимо существование соответствующей международной правовой или политической основы. Эта основа призвана, с одной стороны, закрепить их в качестве элементов нормативной международной правовой или международной политической системы, а с другой – создать определенные условия для их регулирующего воздействия как на международные отношения, так и на общественные отношения в национальных обществах.

2.3. Во-вторых, отсутствие непосредственной взаимосвязи норм ответственного поведения государств в ИКТ-среде с существующими нормами международного права создают дополнительные препятствия на пути их непосредственной имплементации в национальное законодательство ввиду неопределенности их правового статуса.

2.4. В-третьих, отношение государств к соблюдению принципов Устава ООН и других норм международного права отличается двойственностью. С одной стороны, государства выделяют те виды использования ИКТ, которые не хотели бы допускать по отношению к себе, и, с другой стороны, те виды использования ИКТ, которые они хотели бы разрешить себе по отношению к другим государствам.

2.5. В-четвертых, многообразие подходов к толкованию содержания принципа уважения суверенитета, артикулируемого некоторыми государствами в качестве императивной нормы, в конечном счёте свидетельствует об отсутствии самого правила, которое могло бы применяться в отношении ИКТ. Полифоничность позиций государств по данному вопросу не позволяет предположить возможность достижения консенсуса в процессе применения норм ответственного поведения государств в ИКТ-среде.

2.6. В-пятых, юридически обязательные нормы и принципы международного права, на которых в определенной мере базируется применение норм ответственного поведения (принцип суверенного равенства государств и вытекающий из него принцип невмешательства во внутренние дела, принцип неприменения силы и угрозы силой, принцип надлежащей осмотрительности, нормы международного гуманитарного права и международного права прав человека, а также нормы международной ответственности) имеют несовпадающие сферы применения в пространстве ИКТ-среды.

Вследствие этого, обязательства государств, вытекающие из применимости норм и принципов международного права к отношениям, регулируемым нормами ответственного поведения в области ИКТ-среды, требуют уточнения применительно к каждой норме отдельно.

2.7. В-шестых, представления государств о границах зон ответственности в ИКТ-среде существенно различаются. Одни государства исходят из доктринального толкования этих границ как границ территорий государств, на которых расположены объекты национального сегмента ИКТ-среды (именно к этой категории можно отнести так называемое «Таллинское руководство»), в то время как другие – полагают необходимым консенсуальный подход к решению этого вопроса.

Вследствие этого трудно предположить возможность достижения консенсуса по данному вопросу в процессе применения норм ответственности государств в ИКТ-среде.

2.8. В-седьмых, применению норм ответственного поведения государств в ИКТ-среде в форме имплементации в национальное законодательство препятствует терминологическая несогласованность данных норм с нормами национального законодательства, а также отсутствие правовых оснований для их реализации в системе национального права.

2.9. В-восьмых, особой проблемой применения норм ответственного поведения государств в ИКТ-среде является отсутствие поддержки процесса их применения со стороны международного нормативного технического регулирования. Применение международных технических стандартов может содействовать сбору суверенными государствами согласованной и одинаково понимаемой экспертами информации, необходимой для применения средств мирного разрешения международных споров и опасных ситуаций в ИКТ-среде.

3. ПРЕДЛОЖЕНИЯ ПО РЕШЕНИЮ ПРОБЛЕМ ПРИМЕНЕНИЯ НОРМ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИКТ-СРЕДЕ

3.1. В решении проблем применения норм ответственного поведения в ИКТ-среде предлагается выделить следующие основные задачи.

3.2. Адаптация норм и принципов международного права к регулированию отношений в области применения ИКТ и функционирования глобальной информационной инфраструктуры в рамках ИКТ-среды как нового пространства международного сотрудничества.

3.2.1. Адаптация норм и принципов международного права должна способствовать, с одной стороны, достижению устойчивого развития национальных обществ на основе использования потенциала ИКТ во всех сферах жизнедеятельности человека, а с другой – поддержанию международного мира и безопасности в условиях возникновения инцидентов в ИКТ-среде.

При этом необходимо учитывать, что инциденты в ИКТ-среде, равно как и нарушения норм ответственного поведения возникают, в основном, вследствие злонамеренной и вредоносной деятельности некоторых государств и иных субъектов против критически важной информационной инфраструктуры, направленной на достижение военных, террористических и преступных целей на национальном, региональном и глобальном уровнях.

3.2.2. В рамках адаптации норм и принципов международного права к применению в ИКТ-среде необходимо осуществить следующее:

- международное правовое закрепление границ зон ответственности государств в ИКТ-среде;
- уточнение международных обязательств государств в ИКТ-среде, вытекающих из:
- норм и принципов международного права, и, в частности, из принципов суверенного равенства, разрешения международных споров мирными средствами, воздержания от угрозы силой или ее применения против территориальной неприкосновенности или политической независимости государств, уважения прав человека, невмешательства во внутренние дела других государств;
- международных обязательств, обусловленных применением норм ответственного поведения государств в ИКТ-среде;
- обязательств в области обеспечения безопасности критически важной инфраструктуры.

Кроме того, представляется важным уточнение обязательств государств в области обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, а также создание системы компетентных координаторов на политическом и техническом уровнях и определение порядка их взаимодействия в целях обеспечения безопасного использования и устойчивого функционирования ИКТ-среды.

3.3. Развитие на основе политических соглашений государств и международных организаций отдельных норм международного права, устанавливающих международные обязательства государств по процедуре имплементации норм ответственного поведения в ИКТ-среде в национальное законодательство, а также по сотрудничеству в согласовании правовых механизмов регулирования соответствующих групп общественных отношений с учетом различия терминологии, используемой в национальном законодательстве для описания этих отношений.

3.4. Организация сотрудничества в области развития системы международных технических стандартов, устанавливающих порядок размещения информации, необходимой для применения мирных средств разрешения споров и ситуаций. Принятие таких стандартов создаст условия для повышения безопасности использования ИКТ, в том числе, на объектах критически важных инфраструктур.

4. ОСНОВНЫЕ НАПРАВЛЕНИЯ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В ЦЕЛЯХ ПРИМЕНЕНИЯ НОРМ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИКТ-СРЕДЕ

4.1. Применение норм ответственного поведения государств в ИКТ-среде имеет целью сохранение на основе сотрудничества государств открытой, безопасной, стабильной, доступной и мирной ИКТ-среды, имеющей важное значение для устойчивого развития современного общества.

4.2. Выделяются следующие основные направления международного сотрудничества в области применения норм ответственного поведения государств в ИКТ-среде:

- формирование общего понимания содержания норм ответственного поведения государств в ИКТ-среде, а также процессуальных механизмов применения этих норм (включая, вопросы установления и поддержания международного правового режима безопасности критически важной инфраструктуры), а также применения мирных средств разрешения спорных ситуаций в ИКТ-среде;
- делимитация и демаркация границ зон ответственности государств в ИКТ-среде;
- имплементация норм ответственного поведения государств в ИКТ-среде в национальное законодательство;
- обмен информацией, оказание взаимопомощи, преследование лиц, виновных в террористическом и преступном использовании ИКТ;
- развитие системы компетентных координаторов на политическом и техническом уровнях и вовлечение координаторов в координационную сеть.

4.4. Сотрудничество в области формирования общего понимания содержания норм ответственного поведения государств в ИКТ-среде имеет целью предупреждение спорных ситуаций в области толкования применяемых норм, определения предмета нормативного регулирования, а также общего понимания содержания принимаемых государствами обязательств.

К числу понятий, используемых в нормах ответственного поведения государств в ИКТ-среде и не имеющих однозначного толкования, можно отнести, например: «международно-противоправные деяния с использованием

ИКТ»; «вредоносное использование ИКТ»; «террористическое и преступное использование ИКТ», «злонамеренные программные и технические средства ИКТ», «скрытые вредоносные функции».

Добросовестному применению норм способствовало бы также:

- уточнение видов деятельности государств в сфере ИКТ, относимых к «злонамеренным», «заведомо противоречащим международному праву», «наносящим преднамеренный ущерб критически важной инфраструктуре»;
- достижение договоренности по вопросам: классификации мер, принимаемых государством для защиты своей критически важной инфраструктуры в качестве «надлежащих»; выбора критериев «разумности» мер обеспечения целостности каналов поставки в сфере ИКТ.

4.5. Предупреждению возникновения спорных ситуаций способствовало бы также уточнение обязательств государств в области применения норм ответственного поведения государств, регулирующее воздействие которых направлено на запрещение:

- использования своей территории для совершения противоправных деяний, для распространения злонамеренных программных и технических средств в сфере ИКТ, а также средств, обладающих скрытыми вредоносными функциями;
- деятельности, противоречащей обязательствам по международному праву, а также деятельности, призванной нанести ущерб информационным системам уполномоченных групп экстренного реагирования на компьютерные инциденты другого государства.

Достижению этой цели может также способствовать проработка процессуальных вопросов реализации этих норм (включая вопросы обследования объектов ИКТ-среды) и сбора информации, необходимой для мирных средств разрешения международных спорных ситуаций, связанных с инцидентами в ИКТ-среде, в том числе оказывающих влияние на безопасность функционирования критически важной инфраструктуры.

4.6. Сотрудничество в области согласования процедур и механизмов осуществления демаркации и делимитации границ зон ответственности государств в ИКТ-среде является одним из условий возможности применения норм ответственного поведения государств на основе «суверенитета государств, международных норм и принципов, проистекающих из суверените-

та»¹⁰, а также применения средств мирного разрешения международных споров в этой области.

4.6.1. С учетом особенностей ИКТ-среды как глобальной составляющей информационной сферы, включающей взаимосвязанные сети инфраструктуры информационных технологий, делимитация могла бы заключаться в закреплении в международном договоре уникальных цифровых идентификаторов объектов ИКТ-среды, обеспечение безопасности использования которых осуществляется на основе государственного суверенитета.

4.6.2. Демаркация границы зоны ответственного поведения государства в ИКТ-среде могла бы заключаться в следующем:

- оснащение объектов национальной зоны ответственного поведения специальным программным обеспечением и техническим оборудованием, применение которого создаст условия для поддержания установленного правового режима границы зоны ответственности;
- установление международного правового режима безопасности объектов информационной инфраструктуры, оказывающих влияние на функционирование критически важной инфраструктуры.

4.6.3. В рамках правового режима зоны ответственного поведения государства можно было бы закрепить нормативный механизм соблюдения обязательств по нормативно-техническому регулированию отношений в области предупреждения и пресечения, вытекающих из норм ответственного поведения государств в ИКТ-среде, и, в частности, обязательств в области недопущения:

- противоправной деятельности в ИКТ-среде с учетом положений морского, воздушного и космического права;
- деятельности «заведомо противоречащей международному праву» и «наносщей преднамеренный ущерб критически важной инфраструктуре»;
- «международно-противоправных деяний с использованием ИКТ» и «вредоносного использования ИКТ, способного создать условия для нарушения международного мира и безопасности», «террористического и преступного использования ИКТ».

Кроме того, аналогичным образом можно было бы закрепить нормативный механизм оказания помощи государствам, критически важная

¹⁰ Доклад ГПЭ ООН (2015), П.27

инфраструктура которых становится объектом злонамеренных действий и другой деятельности, не способствующей поддержанию международного мира и безопасности.

4.7. Сотрудничество в области имплементации норм ответственного поведения государств в ИКТ-среде в национальное законодательство могло бы содействовать созданию условий для гармонизации этих норм с нормами национального права, регулируемыми отношения в области информационной деятельности в различных сферах общественной жизни.

Это сотрудничество должно базироваться, с одной стороны, на принципе добровольности принятия международных обязательств¹¹, а с другой – на императивной норме международного права, устанавливающей для государств «невозможность ссылаться на положения своего внутреннего права в качестве оправдания для невыполнения им договора»¹².

4.8. Сотрудничество в области обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, является относительно новым направлением взаимодействия государств и других субъектов международного права. В настоящее время это сотрудничество целесообразно сосредоточить на содействии продвижению проекта конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях.

4.9. Сотрудничество в области развития системы компетентных координаторов на политическом и техническом уровнях и вовлечение координаторов в координационную сеть могло бы иметь целью обеспечение надёжной и прямой связи между государствами в целях предотвращения и урегулирования серьезных инцидентов в сфере использования ИКТ и ослабления напряженности в кризисных ситуациях.

Коммуникация между контактными пунктами, осуществляемая под эгидой уполномоченной международной организации (например, Международный Союз Электросвязи) могла бы помочь снизить напряженность и предотвратить недопонимание, которые могут возникнуть в результате инцидентов в сфере использования ИКТ, в том числе затрагивающих критически важную инфраструктуру и имеющих национальное, региональное или глобальное значение.

¹¹ Венская конвенция о праве международных договоров. 1969 г., Ст. 6

¹² Там же. Ст. 27

Государства могли бы в рамках этого направления сотрудничества расширить использование контактных центров для обмена информацией и оказания помощи в эффективном управлении инцидентами в сфере использования ИКТ, а также в содействии урегулированию таких инцидентов¹³.

По существу, речь может идти о создании специализированного механизма (платформы доверия) практического взаимодействия государств по политическим, нормативным и техническим вопросам применения мирных средств разрешения спорных ситуаций в ИКТ-среде таким образом, чтобы «не подвергать угрозе международный мир, безопасность и справедливость»¹⁴.

ЗАКЛЮЧЕНИЕ

В настоящем реферативном материале отмечено, что угрозы злонамеренного использования ИКТ, в том числе в военных и террористических целях, создают значительный риск для международной безопасности и стабильности развития общества, а также для безопасности и благополучия отдельных лиц.

Показано, что перспективным направлением снижения этого риска могло бы стать применение норм ответственного поведения государств в ИКТ-среде (доклады Групп правительственных экспертов 2015 и 2021 гг.), в качестве обязательных норм международного права.

Отмечено, что на пути применения норм ответственного поведения в ИКТ-среде государствами возникают проблемы, обусловленные отсутствием:

- общего понимания содержания международных обязательств государств в области применения ИКТ и использования ИКТ-среды;
- признанных международным сообществом границ зон ответственности государств в ИКТ-среде;
- правовых оснований для имплементации норм ответственного поведения государств в ИКТ-среде в национальное законодательство;
- правовых и иных нормативных оснований для применения некоторых норм ответственного поведения государств.

Подчеркнуто, что возникновение выделенных проблем обусловлено, прежде всего, принципиальными отличиями:

- ИКТ-среды от традиционных пространств международного сотрудничества,
- норм ответственного поведения государств в ИКТ-среде от норм и принципов международного права;
- объектов отношений (информация и ИКТ), регулируемых нормами ответственного поведения государств в ИКТ-среде, от объектов отношений в традиционных областях международного сотрудничества;
- процессов обработки информации на объектах ИКТ-среды, наблюдение которых независимыми экспертами не представляется возможным («ненаблюдаемость»), от процессов деятельности субъектов в традиционных пространствах государственного суверенитета, допускающих возможность такого наблюдения.

Предложено расширять международное сотрудничество в целях содействия созданию условий для применения норм ответственного поведения государств в ИКТ-среде в качестве средства нормативного правового регулирования международных отношений.

¹³ Доклад ГПЭ ООН (2021) П.76

¹⁴ Ст. 2 п. 3 Устава ООН.

AUTHORS' TEAM

1. **Streltsov Anatoly Alexandrovich** – Doctor of Law, Doctor of Technical Sciences, Prof., head of work
2. **Kapustin Anatoly Yakovlevich** – Doctor of Law, Prof.
3. **Smirnov Alexander Alexandrovich** – Candidate of Law
4. **Polyakova Tatyana Anatolyevna** – Doctor of Law, Prof.
5. **Kasenova Madina Baltashevna** – Doctor of Law, Prof.
6. **Rusinova Vera Nikolaevna** – Doctor of Law, Prof.
7. **Shinkaretskaya Galina Georgievna** – Doctor of Law, Prof.
8. **Zharova Anna Konstantinovna** – Doctor of Law, Associate Professor
9. **Pilyugin Pavel Lvovich** – Candidate of Technical Sciences, Associate Professor
10. **Kalitsev Alexander Evgenievich**
11. **Gorzhaltsan Vladimir Akhilovich**
12. **Gerasimov Andrey Vasilyevich**
13. **Markov Alexey Sergeevich** – Doctor of Technical Sciences, Prof.
14. **Miloslavskaya Natalya Georgievna** – Doctor of Technical Sciences, Prof.
15. **Miroshnikov Boris Nikolaevich** – Candidate of Law
16. **Panin Alexander Vyacheslavovich**
17. **Korotkov Sergey Vasilievich** – Candidate of Military Sciences
18. **Boyko Konstantin Sergeevich**
19. **Volkova Svetlana Gennadievna**

FOREWORD

Digital technologies in the 21st century have become an integral attribute of almost all aspects of the life of national societies and international cooperation. The safe use of the global environment of information and communication technologies, as well as the sustainable functioning of its national segments in the modern world, is a condition for maintaining international peace and security.

At the same time, the ongoing «digital transformation» of human life and humanity also creates new risks. The global information space is increasingly turning into a field of information confrontation between the political forces of society, unfair competition between commercial organizations, and tough conflict relations between States. The global environment of information and communication technologies is actively used by international terrorists and organized crime.

In this regard, the initiative of Russian experts, supported by the Association, to study the problems of applying the norms of responsible behavior of States in the ICT environment seems extremely timely.

The results of the conducted research are presented in this abstract material and suggested for discussion at the third substantive session of the UN Open-ended Working Group on Security Issues in the Use of Information and Communication Technologies and Information and Communication Technologies themselves 2021–2025.

I am sure that the discussion of the results of the study by Russian experts will contribute to the formation of a new level of understanding of the problem of legal support for international information security.

*President of the National Association for International Information Security,
Advisor to the Secretary of the Security Council of the Russian Federation,
Corresponding Member of the Academy of Cryptography
of the Russian Federation*

Vladislav Sherstyuk

INTRODUCTION

The active development of information and communication technologies (ICT) and the market for ICT products, the global information infrastructure, the expansion of the use of these technical resources for the provision of communication and information services, as well as the increase in the number of users of these services and ICT products in various fields of activity, are important factors in changing lives of the society. These processes, on the one hand, contribute to the emergence of a new environment for human life – the environment of information and communication technologies (hereinafter referred to as the ICT environment), and on the other hand, create conditions for the formation of a global information society.

In the information society, it is expected that everyone will have the opportunity to «create, access, use and share information and knowledge», and that individuals, communities and peoples will have «the opportunity to realize their full potential by contributing to their sustainable development and improving the quality of their life»¹.

The level of accessibility of ICT, the readiness of citizens, organizations and the State to use these technologies in practical activities become indicators of changes in the socio-cultural conditions of people's lives and become symbols of a new information «dimension» of this life².

In the information society, the security of using the ICT environment is becoming one of the most important factors for sustainable development³. While the malicious use of ICT by unscrupulous States and other subjects in international life creates significant risks for «international security and stability, economic and social development, for the security of the well-being of individuals»⁴.

As the results of the work of the UN General Assembly show, the member States of the international community are paying more and more attention to

¹ Declaration of principles. Building an information society is a global challenge in the new millennium. World Summit on the Information Society. December 12, 2003. item 1. WSIS-03/GENEVA/DOC/4-R

² Information Society in the Russian Federation. Statistical collection. National Research University «Higher School of Economics». Moscow, 2017.

³ Declaration of principles. Building an information society is a global challenge in the new millennium. World Summit on the Information Society. December 12, 2003. item 9. <https://www.itu.int/net/wsis/index-ru.html>

⁴ Report of the Group of Governmental Experts on Advancing Responsible Behavior of States in Cyberspace of ICT Environment in the Context of International Security (Report A/76/135, 2021). item 6

the issues of ensuring the security of the use of ICT, the sustainability of the functioning of the global ICT environment.

Ensuring the security of the use of the global ICT environment based on the application of the norms and principles of international law faces a number of objective difficulties. This is the reason for the proposal of a number of member States of the Shanghai Cooperation Organization to propose rules of conduct in the field of ensuring international information security⁵ for consideration at the UN General Assembly. The rules proposed by the States of the Shanghai Cooperation Organization created a methodological basis for the preparation by the Groups of Governmental Experts (2015, 2021) of the norms, rules and principles (hereinafter referred to as norms) of responsible behavior of States in the ICT environment⁶ as well as the materials of the 2021 UN Open Ended Working Group⁷.

According to the international community, the application of the norms of responsible behavior of States in the ICT environment, in parallel with the application of the principles and norms of international law, can contribute to strengthening international peace and security.

In order to facilitate discussion at the site of the UN Open-ended Working Group on the application of the norms of responsible behavior of States in the ICT environment, the National Association for International Information Security has prepared this abstract.

The material reflects the results of an expert study of the problems of the practical application of these norms of responsible behavior in the activities of States conducted by the National Association.

According to Russian experts, the success of applying the norms of responsible behavior as a means of regulating international relations in the ICT environment will depend on the solution of a number of complex problems, primarily due to the special properties of this new space for international cooperation.

⁵ Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General of the United Nations (A/66/359), Letter dated 9 January 2015 from the Permanent Representatives of Kazakhstan, China, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General of the United Nations (A/69/723)

⁶ Report of the Group of Governmental Experts on Developments in Information and Telecommunications in the Context of International Security (A/70/174), Report of the Group of Governmental Experts on Advancing Responsible Behavior of States in Cyberspace in the Context of International Security (A/76/135)

⁷ Final Keynote Report of the United Nations Open Working Group on Advances in Information and Telecommunications in the Context of International Security, March 10, 2021. A/AC.290/2021/CRP.2

1. INFORMATION AND COMMUNICATION TECHNOLOGY ENVIRONMENT AS A SPACE FOR COOPERATION

1.1. ICT environment is formed by a combination of information infrastructure (information located on electronic computing devices; digital ICT of information processing and communication networks) and users using this infrastructure to participate in a variety of public relations. The formation of the national segment of the ICT environment is an important factor in the development of Russian society and the state.

The information and communication infrastructure is the basis of the national segment of the ICT environment and, at the same time, one of the key components of the infrastructure of the Russian Federation.

The security of using the national segment of the ICT environment and the stability of the functioning of the national information infrastructure (information security) have a significant impact on the national security of the Russian Federation.

1.2. The national segment of the ICT environment is an integral part of the global ICT environment, the technical basis of which is global communication networks and the global information and communication network Internet.

The malicious and harmful activities of certain States and other entities carried out for military, terrorist and criminal purposes at the national, regional and global levels are becoming an increasingly serious threat to international peace and security.

Of particular concern are malicious activities in the use of ICTs that affect critical infrastructure. The security and sustainability of critical infrastructure in today's society depend on the security of ICT use. The critical importance of this infrastructure is due to its use for the provision of basic services to the population, for ensuring the general availability and integrity of the Internet, as well as for the activities of the civil society organizations in the economic, social, political and cultural spheres, for the effective operation of government bodies.

In the near future the importance of the security of using ICT and the sustainability of the functioning of the information infrastructure as factors in ensuring national and international security will increase.

1.3. The ICT environment as a space for international cooperation has properties that fundamentally distinguish it from the properties of traditional spaces for

the implementation of the territorial sovereignty of States and international cooperation (land, sea, air, outer space and subsoil). Among the distinctive properties of the ICT environment as a space for cooperation are: the special nature of social relations implemented using this space (information relations); special properties of information as an object of processing using ICT (virtuality); the special nature of ways to maintain the functioning of the ICT environment as a space for the implementation of human information activities (partnership between the State and business); a special legal status of a person as a subject of information activity, including in the ICT environment (freedom of information activity).

1.4. The norms of responsible behavior of States in the ICT environment, can become a means of legal regulation of international relations subject to their consolidation in an international agreement. At present these norms are recommendatory, legally non-binding rules of conduct for States listed in the reports of the Groups of Governmental Experts⁸ and recommended to States for consideration by resolutions of the UN General Assembly⁹.

These rules of behavior of States arise from the general principles of public morality and supplement the norms of international and national law as well as the «soft law» norms enshrined in international political agreements.

The norms of responsible behavior of States can, after their consolidation in an international agreement, be taken into account in the interpretation of existing international legal norms, contribute to the emergence of new international customs and serve as a guideline in the conclusion of international treaties.

1.5. The application of the norms of responsible behavior of States in the ICT environment is one of the forms of implementation of international obligations of States carried out taking into account the norms and principles of international law and national legislation.

2. PROBLEMS OF APPLICATION OF THE NORMS OF RESPONSIBLE BEHAVIOR OF STATES IN THE ICT ENVIRONMENT

2.1. The application of the norms of responsible behavior of States in the ICT environment to regulate international relations and public relations that fall under national jurisdiction faces a number of fundamental problems.

⁸ A/70/235, A/76/135

⁹ A/70/134, A/75/240

2.2. Firstly, the norms of responsible behavior of States in the ICT environment do not follow directly from the existing norms of international law, i. are not provisions of the *lex lata* of public international law. These norms are aimed at clarifying the interpretation of existing norms of international law in relation to relations in the ICT environment, as well as at expanding the composition of the international regulatory system that regulates activities in the field of the use of ICT.

As a result, the existence of an appropriate international legal or policy framework is necessary for the application of the norms of responsible behavior of States in the ICT environment. This framework is intended, on the one hand, to consolidate them as elements of the normative international legal or international political system, and on the other hand, to create certain conditions for their regulatory impact both on international relations and on public relations in national societies.

2.3. Secondly, the lack of the direct relationship between the norms of responsible behavior of States in the ICT environment and the existing norms of international law create additional obstacles to their direct implementation in national legislation due to the uncertainty of their legal status.

2.4. Thirdly, the attitude of States to the observance of the principles of the UN Charter and other norms of international law is ambivalent. On the one hand, States identify those uses of ICT that they would not like to allow in relation to themselves, and, on the other hand, those types of use of ICT that they would like to allow in relation to other States.

2.5. Fourthly, the variety of approaches to interpreting the content of the principle of respect for sovereignty, articulated by some States as an imperative norm, ultimately indicates the absence of the very rule that could be applied to ICT. The polyphony of States' positions on this issue does not allow us to assume the possibility of reaching a consensus in the process of applying the norms of responsible behavior of States in the ICT environment.

2.6. Fifthly, legally binding norms and principles of international law, on which the application of norms of responsible behavior is based to a certain extent (the principle of sovereign equality of States and the principle of non-intervention in internal affairs arising from it, the principle of non-use of force and threat of force, the principle of due diligence, the norms of international humanitarian law and international human rights law, as well as the norms of international responsibility) have different areas of application in the space of the ICT environment.

As a result, the obligations of States arising from the applicability of the norms and principles of international law to relations governed by the norms of responsible behavior in the field of the ICT environment require clarification in relation to each norm separately.

2.7. Sixth, the ideas of States about the boundaries of the zones of responsibility in the ICT environment differ significantly. Some States proceed from the doctrinal interpretation of these borders as the borders of the territories of the States where the objects of the national segment of the ICT environment are located (the so-called «Tallinn Manual» can be attributed to this category), while others consider it necessary to take a consensual approach to solving this problem.

As a result, it is difficult to imagine the possibility of reaching a consensus on this issue in the process of applying the norms of States' responsibility in the ICT environment.

2.8. Seventh, the application of the norms of responsible behavior of States in the ICT environment in the form of implementation into national legislation is hindered by the terminological inconsistency of these norms with the norms of national legislation, as well as the lack of legal grounds for their implementation in the system of national law.

2.9. Eighth, a special problem of applying the norms of responsible behavior of States in the ICT environment is the lack of support for the process of their application from the side of international normative technical regulation. Application of international technical standards makes it possible to collect information coordinated and equally understood by experts, necessary for the use of means of peaceful resolution of international disputes and dangerous situations related to incidents in the ICT environment.

3. PROPOSALS FOR SOLVING THE PROBLEMS OF APPLYING THE NORMS OF RESPONSIBLE BEHAVIOR OF STATES IN THE ICT ENVIRONMENT

3.1. In solving the problems of applying the norms of responsible behavior in the ICT environment, it is proposed to single out the following main tasks.

3.2. Adaptation of the norms and principles of international law to the regulation of relations in the field of ICT application and the functioning of the global information infrastructure within the ICT environment as a new space for international cooperation.

3.2.1. Adaptation of the norms and principles of international law should contribute, on the one hand, to the achievement of sustainable development of national societies based on the use of the potential of ICT in all spheres of human life, and on the other hand, to the maintenance of international peace and security in the event of incidents in the ICT environment.

At the same time, it should be taken into account that incidents in the ICT environment, as well as violations of the norms of responsible behavior, arise mainly as a result of the malicious and harmful activities of some States and other entities against critical information infrastructure aimed at achieving military, terrorist and criminal goals on national, regional and global levels.

3.2.2. As part of the adaptation of the norms and principles of international law for application in the ICT environment, it is necessary to carry out the following:

- international legal consolidation of the boundaries of the zones of responsibility of States in the ICT environment;
- clarification of the international obligations of States in the ICT environment arising from:
- the norms and principles of international law, and, in particular, from the principles of sovereign equality, the resolution of international disputes by peaceful means, refraining from the threat or use of force against the territorial integrity or political independence of States, respect for the human rights, non-interference in the internal affairs of other States;
- international obligations arising from the application of the norms of responsible behavior of States in the ICT environment;
- obligations to ensure the security of critical infrastructure.

Besides, it seems to be important to clarify the obligations of States in the field of information exchange, mutual assistance, prosecution of persons guilty of terrorist and criminal use of ICT as well as to create a system of competent coordinators at the political and technical levels and determine the order of their interaction in order to ensure the safe use and sustainable functioning of the ICT environment.

3.3. Development on the basis of political agreements of States and international organizations of certain norms of international law, establishing the international obligations of States on the procedure for implementing the norms of responsible behavior in the ICT environment into national legislation, as well as on cooperation in agreeing legal mechanisms for regulating the relevant groups

of public relations taking into account the difference in terminology used in national legislation to describe these relationships.

3.4. Organization of cooperation in the field of the development of a system of international technical standards establishing the order to place information necessary to implement peaceful means to resolve disputes and situations. The adoption of such standards is to create conditions to improve security of ICT use including the objects of critically important infrastructures.

4. MAIN DIRECTIONS OF INTERNATIONAL COOPERATION IN ORDER TO APPLY THE NORMS OF RESPONSIBLE BEHAVIOR OF STATES IN THE ICT ENVIRONMENT

4.1. The application of the norms of responsible behavior of States in the ICT environment is aimed at maintaining, on the basis of cooperation between States, an open, safe, stable, accessible and peaceful ICT environment, which is important for the sustainable development of modern society.

4.2. The main areas of international cooperation in the field of application of the norms of responsible behavior of States in the ICT environment are as follows:

- formation of a common understanding of the content of the norms of responsible behavior of States in the ICT environment, as well as the procedural mechanisms for the application of these norms (including the issues of establishing and maintaining an international legal regime for the security of critical infrastructure), as well as the use of peaceful means of resolving disputes in the ICT environment;
- delimitation and demarcation of the boundaries of the zones of responsibility of States in the ICT environment;
- implementation of the norms of responsible behavior of States in the ICT environment into national legislation;
- exchange of information, provision of mutual assistance, prosecution of persons guilty of terrorist and criminal use of ICT;
- development of a system of competent coordinators at political and technical levels and involvement of coordinators in the coordinating network.

4.4. Cooperation in the field of forming a common understanding of the content of the norms of responsible behavior of States in the ICT environment

is aimed at preventing disputes related to the interpretation of the applicable norms, the definition of the subject of regulation as well as general understanding of the content of the obligations assumed by the States.

The concepts used in the norms of responsible behavior of States in the ICT environment and not having an unambiguous interpretation include, for example: «internationally wrongful acts using ICT»; «malicious use of ICT»; «terrorist and criminal use of ICT», «malicious ICT software and hardware», «hidden malicious functions».

The conscientious application of the norms would also be facilitated by:

- clarifying the types of activities of States in the field of ICT, classified as «malicious», «knowingly contrary to international law» and «inflicting deliberate damage to critical infrastructure»;
- reaching an agreement on: the classification of measures taken by the State to protect its critical infrastructure as «appropriate»; «reasonable» measures to ensure the integrity of ICT supply chains.

4.5. The clarification of the obligations of States in the field of application of the norms of responsible behavior of States would also help to prevent the occurrence of disputes, the regulatory effect of which is aimed at prohibiting:

- using proper territory to commit illegal acts, to distribute malicious software and hardware in the field of ICT, as well as tools with hidden malicious functions;
- activities contrary to obligations under international law, as well as activities designed to damage the information systems of authorized emergency response teams to computer incidents of another State.

The achievement of this goal can also be facilitated by the elaboration of procedural issues for the implementation of these norms (including the issues of surveying objects of the ICT environment) and the collection of information necessary for peaceful means of resolving international disputes related to incidents in the ICT environment, including objects of the ICT environment, affecting the safety of critical infrastructure operation.

4.6. Cooperation in the field of harmonization of procedures and mechanisms for the implementation of the demarcation and delimitation of the boundaries of the zones of responsibility of States in the ICT environment is one of the conditions for the applicability of the norms of responsible behavior of States

based on «the sovereignty of States, international norms and principles arising from sovereignty»¹⁰, as well as means of peaceful resolution of international disputes to relations in this area.

4.6.1. Taking into account the peculiarities of the ICT environment as a global component of the information sphere, including interconnected networks of information technology infrastructure, delimitation could consist in fixing unique digital identifiers of objects of the ICT environment in an international treaty, the secure use of which is carried out on the basis of State sovereignty.

4.6.2. The demarcation of the border of the zone of responsible behavior of the State in the ICT environment could be the following:

- equipping the objects of the national zone of responsible behavior with special software and technical equipment, the use of which will create conditions for maintaining the established legal regime of the border of the zone of responsibility;
- establishing of the international legal regime for the security of information infrastructure objects, affecting the operation of critical infrastructure.

4.6.3. Within the framework of the legal regime of the zone of responsible behavior of the State, it would be possible to consolidate the regulatory mechanism for compliance with obligations on the normative and technical regulation of relations arising from the norms of responsible behavior of States in the ICT environment in the field of prevention of the following:

- illegal activities in the ICT environment, taking into account the provisions of the maritime, air and space law;
- activities «knowingly contrary to international law» and «deliberately damaging critical infrastructure»;
- committing «internationally wrongful acts using ICT» and «malicious use of ICT capable of creating conditions for the violation of international peace and security», «terrorist and criminal use of ICT».

In addition, a normative mechanism for providing assistance to States whose critical infrastructure becomes the target of malicious acts and other activities that do not contribute to the maintenance of international peace and security could be fixed in a similar way.

4.7. Cooperation in the field of implementation of the norms of responsible behavior of States in the ICT environment in national legislation could help

¹⁰ UN GGE Report (2015), item 27

create conditions for harmonizing the norms of responsible behavior and the norms of national law governing relations in the field of information activities in various spheres of public life.

This cooperation should be based, on the one hand, on the principle of voluntariness in the fulfillment of international obligations¹¹, and on the other hand, on the imperative norm of international law, which establishes for States «the impossibility of referring to the provisions of their internal law as an excuse for not fulfilling a treaty»¹².

4.8. Cooperation in the field of information exchange, mutual assistance, prosecution of persons guilty of terrorist and criminal use of ICT is a relatively new area of interaction between States and other subjects of international law. At present, this cooperation should be focused on promoting the draft United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

4.9. Cooperation in the development of a system of competent coordinators at the political and technical levels and the involvement of coordinators in the coordination network could be aimed at ensuring reliable and direct communication between States in order to prevent and resolve serious incidents in the use of ICT and reduce tension in crisis situations.

Communication between contact points, carried out under the auspices of an authorized international organization (for example, the International Telecommunication Union) could help reduce tension and prevent misunderstandings that may arise from incidents in the use of ICT, including those affecting critical infrastructure and having a national, regional or global value.

States could, within the framework of this area of cooperation, expand the use of contact centers to exchange information and assist in the effective management of incidents in the use of ICT, as well as in facilitating the resolution of such incidents¹³.

In essence, we can talk about creating a specialized mechanism (platform of trust) for the practical interaction of States on political, regulatory and technical issues of using peaceful means of resolving disputes in the ICT environment in such a way as not to «endanger international peace, security and justice»¹⁴.

¹¹ Vienna Convention on the Law of Treaties. 1969, page 6

¹² Ibid. Page 27

¹³ UN GGE Report (2021), item 76

¹⁴ Art. 2, paragraph 3, of the UN Charter.

CONCLUSION

This abstract material notes that the threats of malicious use of ICTs, including for military and terrorist purposes, pose a significant risk to international security and stability, the economic and social development of society, and the security and well-being of individuals.

It is shown that one of the promising ways to reduce this risk could be the application of the norms of responsible behavior of States in the ICT environment (the reports of the Groups of Governmental Experts in 2015 and 2021) as legally binding.

It is noted that on the way to the application of the norms of responsible behavior in the ICT environment by States problems arise due to the lack of:

- a common understanding of the content of the international obligations of States in the field of the use of ICT and the use of the ICT environment;
- recognized by the international community as the boundaries of the zones of responsibility of States in the ICT environment;
- legal grounds for the implementation of the norms of responsible behavior of States in the ICT environment in national legislation;
- legal and other regulatory grounds for the application of certain norms of responsible behavior of States.

It is emphasized that the emergence of the above mentioned problems is primarily due to the fundamental differences:

- the ICT environment and traditional spaces of international cooperation;
- the norms of responsible behavior of States in the ICT environment and the norms and principles of international law;
- the objects of relations (information and ICT) governed by the norms of responsible behavior of States in the ICT environment and the objects of relations in traditional fields of international cooperation;
- the information processing at the objects of the ICT environment, the observation of which by independent experts is not possible (non-observability) and subjects activity in traditional spaces of state sovereignty, allowing the possibility of such observation.

It is proposed to expand international cooperation in order to promote the creation of conditions for the application of the norms of responsible behavior of States in the ICT environment as a means of legal regulation of international relations.

