Институт проблем информационной безопасности
Московского государственного университета имени М.В.Ломоносова

А.А.Стрельцов, Р.А.Шаряпов, В.В.Ященко

Краткий комментарий и предложения к п.13 Доклада Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (Семидесятая сессия Генеральной Ассамблеи ООН, 22 июля 2015 года, A/70/174)

«Рекомендации в отношении добровольных и необязательных норм, правил или принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды»

Под редакцией
члена-корреспондента
Академии криптографии Российской Федерации
В.П.Шерстюка

г.Москва
2016

Предлагаемый краткий комментарий и предложения касаются рекомендаций в отношении добровольных и необязательных норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Рекомендации предложены Группой правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (п. 13 доклада Семидесятой сессии Генеральной Ассамблеи ООН, 22 июля 2015 года, A/70/174).

Краткий комментарии и предложения подготовлены с учетом положений Устава ООН, Декларации о принципах международного права[1], Конвенции о праве международных договоров[2], других источников международного права.

В материале изложены взгляды авторов на содержание сформулированных Группой правительственных экспертов норм, правил и принципов с позиции их использования совместно с положениями принципов и норм международного права при регулировании международных отношений в ИКТ-сфере, а также предложения по возможным направлениям развития данных норм, правил и принципов.

Краткий комментарий и предложения предназначены для популяризации норм, правил и принципов ответственного поведения государства в ИКТ-среде в сообществе специалистов в области международного права, занимающихся вопросами его применения к ИКТ-среде, научных работников и иных граждан, интересующихся развитием международного права в условиях глобализации информационного пространства.

[1] Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций. Принята резолюцией 2625 (XXV) Генеральной Ассамблеи ООН от 24 октября 1970 года.

[2] Венская конвенция о праве международных договоров. Принята 23 мая 1969 года.

1. Общие положения

1.1. Ответственное поведение государств заключается, прежде всего, в соблюдении и уважении принципов и норм международного права, источниками которого являются: общие и специальные международные конвенции; международный обычай как доказательство всеобщей практики, признанной в качестве правовой нормы; общие принципы права, признаваемые цивилизованными нациями. В качестве вспомогательных средств для определения правовых норм выступают решения Международного Суда (для участвующих в деле сторон и лишь по данному делу) и доктрины наиболее квалифицированных специалистов по публичному праву.

Применение понятия «ответственное поведение государств» к деятельности государств в ИКТ-среде затрудняется отсутствием общепринятой терминологии, принципов и норм международного права для международных отношений в ИКТ-среде.

1.2. Необходимость адаптации терминологии, принципов и норм международного права к международным отношениям в ИКТ-среде обусловлена следующими факторами:

- интенсивное развитие ИКТ-среды как относительно самостоятельной сферы международных отношений, оказывающей все возрастающее влияние на развитие современного общества;
- существенные отличия ИКТ-среды от других сфер международных отношений, регулируемых международных правом;
- обусловленные этими отличиями сложности применения терминологии, принципов и норм международного права к международным отношениям в ИКТ-среде.

1.3. Термин «ИКТ-среда» в универсальных международных актах не раскрывается.

Сокращением «ИКТ» в технической и общественно-политической литературе обычно обозначают «информационно-коммуникационные технологии», которые представляют собой процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации, а также способы осуществления таких процессов и методов[3] [4].

---

[3] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

[4] 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,

ИКТ-среда образуется совокупностью объектов, относящихся к ИКТ и обеспечивающих применение этих технологий. Множество общественных отношений, в том числе и международных, по поводу деятельности в ИКТ-среде образуют сферу ИКТ.

1.4. В ИКТ-среде выделяются две основные составляющие - «киберпространство» и «пространство выражения мнений, свободы ассоциаций, частной жизни и других прав человека, образования, пропаганды идей (в том числе религиозных и политических, пропагандирующих ненависть, подстрекающих к дискриминации и насилию) в Интернете»[5], другими словами - «пространство сведений и смыслов».

1.5. Термин «киберпространство» может раскрываться как «электронная (включая фотоэлектронную и пр.) среда, в (посредством) которой информация создается, принимается, хранится, обрабатывается и уничтожается»[6]. Термин «электронная среда» рассматривается как совокупность систем технических средств и коммуникационных устройств, обеспечивающих распространение электромагнитных волн по проводным и беспроводным каналам связи для передачи информации (средства связи и коммуникации), а также «технических средств и систем создания, преобразования, передачи, использования и хранения информации», образующих «информационную инфраструктуру» общества.

Часть киберпространства, все объекты которой расположены на данной национальной территории, можно назвать «национальным киберпространством».

В киберпространстве как конструктивная, так и деструктивная (враждебная, агрессивная, противоправная, террористическая) деятельность осуществляются с помощью одних и тех же технологий, на основе которых разрабатываются необходимые средства и инструменты.

Киберпространство обладает свойством глобальности, которое проявляется в интеграции национальных киберпространств в единое киберпространство, обеспечивающее возможность:

- информационного взаимодействия субъектов, находящихся в различных государствах;

---

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

[5] Резолюция Совета по правам человека A/HRC/RES/26/13 от 14 июля 2014 года «Поощрение, защита и осуществление прав человека в Интернете».

[6] Russia – US Bilateral on Cybersecurity. Critical Terminology foundations. EastWest Institute Worldwise Cybersecurity Initiative, Moscow state university information security institute. November 2013.
http://wiki.informationsecurity.club/lib/exe/fetch.php?media=documents_all:russia-u_s_bilateral_on_terminology_rus.pdf

- использования ИКТ с привлечением ресурсов и объектов, расположенных на территории разных государств.

Глобальность киберпространства поддерживается посредством единых систем цифровой адресации объектов, единых протоколов взаимодействия сетей, вычислительных систем, технических и коммуникационных устройств. Функционирование указанных механизмов обеспечивается специальной, критически важной частью киберпространства, которая называется системой Уникальных идентификаторов Интернета.

1.6. «Пространство сведений и смыслов» может трактоваться как «медиасфера» - совокупность идей, тем, мнений и других нематериальных сущностей, представленная медиатекстами, обладающими признаками важности, значимости для разных групп аудиторий, сиюминутности, злободневности, открытости для многочисленных интерпретаций[7].

Сведения представляют собой результат отражения окружающего мира, в том числе сообщений и данных, в организме человека и могут проявляться в форме его мыслей. При этом «сообщения» представляют собой набор знаков, с помощью которых сведения могут переданы от одного человека другому и восприняты им, а «данные» – сообщения, представленные в форме, доступной для обработки с использованием средств вычислительной техники и коммуникационного оборудования[8].

Термин «смысл» в словарях раскрывается как «внутреннее, логическое содержание (слова, речи, явления), постигаемое разумом, значение»[9]. В то же время представляется возможным раскрытие данного термина как логико-эмоциональное отражение сведений в сознании и «бессознательном» человека, порождающее его интересы и мотивы его поступков.

«Пространство сведений и смыслов» включает как субъективные пространства сведений и смыслов отдельных людей, так и общественные пространства сведений и смыслов.

Субъективное «пространство сведений и смыслов» образуется совокупностью представлений человека об окружающей среде, закономерностях ее развития, а также мыслей, связанных с нуждами, потребностями, интересами и действиями данного человека.

Общественное «пространство сведений и смыслов» образуется совокупностью общих (близких по содержанию) для определенной социальной группы людей представлений об окружающей среде, закономерностях ее развития, а также мыслей, связанных с общими нуждами,

---

[7] Буряк М.А. Медиасфера: концептуализация понятия. Вестник СПбГУ. Сер. 9. 2014. Вып. 2. С. 209.

[8] Стрельцов А.А. Обеспечение информационной безопасности России. М., МЦНМО, 2002.

[9] http://slovarsbor.ru/w/смысл/

потребностями, интересами и согласованными действиями данной группы людей.

1.7. К числу особенностей ИКТ-среды и сферы ИКТ, обусловливающих сложности применения терминологии, принципов и норм международного права к международным отношениям в ИКТ-среде, следует отнести, прежде всего, следующие:

- процессы взаимодействия субъектов в ИКТ-среде происходят в форме процессов протекания потоков электромагнитных импульсов через технические средства, средства вычислительной техники и коммуникационные устройства; субъекты деятельности в ИКТ-среде представлены, как правило, только в виде сетевых адресов или номеров используемых ими устройств (анонимность Интернета), что позволяет субъекту затруднить юридически значимую идентификацию его личности и установление ее отношения к тому или иному государству;

- юридические факты, определяющие возникновение, изменение и прекращение правоотношений между субъектами, существуют в форме электромагнитных импульсов, зафиксированных в какой-то момент времени в устройствах ИКТ-среды; возникновение, изменение и прекращение правоотношений между субъектами, возникающих в связи с наличием юридических фактов, происходит в темпе изменения потоков электромагнитных импульсов; фиксация наличия указанных юридических фактов посредством органов чувств человека невозможна; закрепление необходимых юридических фактов и содержания правоотношений возможно только при использовании системы специальных технических средств и соответствующих методик;

- международное процессуальное право как совокупность принципов и норм, регулирующих порядок осуществления прав и обязанностей субъектов международного права, не адаптировано к регулированию международных отношений в сфере ИКТ;

- использование международных обычаев и общих принципов права, признанных цивилизованными нациями, для регулирования международных отношений в сфере ИКТ, представляется малоперспективным ввиду отсутствия единого понимания некоторых объектов правового регулирования, например, использование ИКТ в качестве средства ведения военных действий.

2. Преамбула п.13 «С учетом существующих и нарождающихся угроз, рисков и факторов уязвимости, а также в развитие оценок и рекомендаций, содержащихся в докладах групп предыдущих созывов за 2010 и 2013 годы, настоящая группа предлагает государствам

рассмотреть следующие рекомендации в отношении добровольных и необязательных норм, правил или принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ –среды»

Комментарий к преамбуле п.13

2.1. Рекомендации Группы по нормам, правилам и принципам ответственного поведения государств в ИКТ-среде изложены в форме положений так называемого «мягкого права».

При этом заявленная в п. 10 Доклада надежда, что «Эти нормы … позволяют международному сообществу давать оценку действиям и намерениям государств» нереальна, пока не будут решены указанные выше (п. 1.7) задачи.

2.2. Предлагаемые нормы, правила и принципы ответственного поведения государств не обеспечиваются принуждением и, следовательно, не являются нормами международного права, но могут рассматриваться как основа при формировании обычных норм международного права для регулирования отношений в сфере ИКТ.

2.3. **Объектом международного правового регулирования** являются международные отношения в области обеспечения открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

2.4. **Предметом международного правового регулирования** являются международные отношения по поводу ответственного поведения государств при осуществлении деятельности в ИКТ-среде.

2.5. Открытость ИКТ-среды означает доступность этой среды для людей, проживающих во всех государствах мира, которая достигается на основе интеграции национальных киберпространств и медиасфер в глобальную ИКТ-среду.

2.6. Безопасность ИКТ-среды означает защищенность субъектов жизнедеятельности общества, использующих ИКТ-среду для решения стоящих перед ними задач, от угроз, рисков и факторов уязвимости, возникающих в ИКТ-среде (см. ч. II Доклада Группы), а также от угроз национальной безопасности каждого из государств, осуществляющих деятельность в ИКТ-среде.

2.7. Стабильность ИКТ-среды означает ее способность содействовать выполнению задач, стоящих перед субъектами жизнедеятельности общества, в условиях нарушения (временного) работоспособности отдельных элементов ИКТ-среды.

2.8. Доступность ИКТ-среды означает постоянную возможность использования ИКТ-среды для удовлетворения законных интересов субъектов жизнедеятельности общества, включая интересы, связанные с осуществлением прав и свобод человека.

2.9. Мирность ИКТ-среды означает:

- использование государствами потенциала ИКТ-среды для мирного разрешения международных споров «таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость»[10];

- неиспользование государствами потенциала ИКТ-среды для «угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с Целями Объединенных Наций»[11].

3. Подпункт а) «в соответствии с целями Устава Организации Объединенных Наций, в том числе касающимися поддержания международного мира и безопасности, государства должны сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности»

Комментарий к подпункту а) п.13

3.1. **Объектом международного правового регулирования** являются международные отношения в области сотрудничества государств.

В соответствии с Декларацией о принципах международного права[12] международное сотрудничество государств для поддержания международного мира и безопасности является одной из целей ООН. В соответствии с принципом международного сотрудничества государства обязаны, независимо от различий в их политических, экономических и социальных системах, сотрудничать друг с другом в различных областях международных отношений с целью поддержания международного мира и безопасности и содействия международной экономической стабильности и прогрессу, общему благосостоянию народов и международному

[10] Устав ООН. Ст. 2(3).
[11] Там же. Ст. 2(4).
[12] Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций. Принята резолюцией 2625 (XXV) Генеральной Ассамблеи ООН от 24 октября 1970 года.

сотрудничеству, свободному от дискриминации, основанной на таких различиях.

3.2. Данный принцип по существу выражает глубинный механизм функционирования ООН, вся деятельность которой в любой области базируется на сотрудничестве государств-членов Организации.

3.3. **Предметом международного правового регулирования** является международное сотрудничество в области укрепления стабильности и безопасности в использовании ИКТ.

3.4. **Цели международного правового регулирования** заключаются в активизации международного сотрудничества по направлениям:

- разработка и осуществление мер по укреплению стабильности и безопасности в использовании ИКТ;
- предупреждение совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности.

3.5. Разработка и осуществление мер по укреплению стабильности и безопасности в использовании ИКТ предполагает совместную деятельность государств по противодействию наиболее опасным угрозам нарушения стабильности и безопасности в использовании ИКТ.

К таким угрозам относятся, прежде всего, следующие две угрозы, указанные в п.п. 4 и 5 Доклада:

«4. Ряд государств занимаются наращиванием потенциала в сфере ИКТ для военных целей. Использование ИКТ в будущих конфликтах между государствами становится более вероятным.

5. 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».

Совместные меры государств, направленные на снижение опасности проявления данных угроз, могут включать:

- политические решения государств об ограничении или отказе от использования ИКТ в качестве силы или угрозы силой в международных отношениях;
- определение и закрепление в универсальном международном договоре перечня критически важных объектов инфраструктуры, защищаемых международным правом от нападений с использованием ИКТ.

3.6. Сотрудничество в области предупреждения совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу

международному миру и безопасности, может быть направлено на разработку и осуществление следующих совместных мер:

- определение и закрепление в универсальном международном договоре признаков действий в сфере ИКТ, которые являются вредоносными или способными создать угрозу международному миру и безопасности;
- принятие государствами обязательства не совершать вредоносные и опасные для дела мира действия в сфере ИКТ;
- создание системы расследования фактов (признаков) нарушения государствами обязательств в области предупреждения совершения вредоносных и опасных для дела мира действий в сфере ИКТ.

4. Подпункт b) «в случае инцидентов в сфере ИКТ государства должны изучить всю соответствующую информацию, в том числе более общий контекст события, проблемы присвоения ответственности в ИКТ-среде, а также характер и масштабы последствий»

Комментарий к подпункту b) п.13

4.1. **Объектом международного правового регулирования** являются международные отношения в области исследования инцидентов в сфере ИКТ.

4.2. В международном праве понятие «инцидент» применяется достаточно широко. Так, понятие «инцидент (международный инцидент)» обычно раскрывается как небольшие или ограниченные действия или авария, результатом которых стал широкий обмен мнениями между двумя или более национальными государствами[13].

Инцидент на море означает событие или последовательность событий иных, чем авария на море, произошедших в непосредственной связи с эксплуатацией судна, которые угрожали или, не будучи предотвращены, могли бы угрожать безопасности судна, людей на судне либо любого иного лица или окружающей среды[14].

В области загрязнения окружающей среды нефтепродуктами термин «инцидент» означает любое происшествие или ряд происшествий одного и

[13] An international incident is a seemingly relatively small or limited action or clash that results in a wider dispute between two or more nation-states: https://en.wikipedia.org/wiki/International_incident

[14] Кодекс международных стандартов и рекомендуемой практики расследования аварии или инцидента на море. 2008.

того же происхождения, результатом которых является ущерб от загрязнения[15].

В области загрязнения морской среды - событие, вызывающее фактический или возможный сброс в море вредного вещества или стоков, содержащих такое вещество[16].

В области транспортировки грузов - любое происшествие или ряд происшествий одного и того же происхождения, результатом которых является ущерб или возникновение серьезной и неизбежной опасности причинения ущерба[17].

В области загрязнения бункерным топливом - любое происшествие или ряд происшествий одного и того же происхождения, в результате которых причинен ущерб от загрязнения или возникла серьезная и неминуемая угроза причинения такого ущерба[18].

В области гражданской авиации для обозначения опасных событий в области эксплуатации летной техники используются два термина[19]: авиационный инцидент и авиационное происшествие.

4.3. С учетом описанной выше структуры ИКТ-среды (см. п.п. 1.4, 1.5, 1.6) инцидент в ней может затрагивать как киберпространство, так и медиасферу.

Инцидент в киберпространстве, как правило, связан с нарушением функционирования составляющих киберпространства - электронной среды создания, сбора, передачи, хранения и обработки информации, технических средств осуществления данных операций, а также информационных систем и систем автоматизированного управления.

Инцидент в медиасфере может быть связан с нарушением конфиденциальности информации, попытками изменения ее значимости для граждан, нарушением свободы слова и выражения мысли, а также злоупотреблением этой свободой.

4.4. **Предметом международного правового регулирования** являются международные отношения по поводу изучения всей информации об инцидентах в сфере ИКТ, включая общий контекст события, проблему

---

[15] Международная конвенция о гражданской ответственности за ущерб от загрязнения нефтью (КГО/CLC). 1969.

[16] Конвенция по защите природной морской среды района Балтийского моря. 1992.

[17] Конвенция о гражданской ответственности за ущерб, причиненный при перевозке опасных грузов автомобильным, железнодорожным и внутренним водным транспортом. 1989.

[18] Международная конвенция о гражданской ответственности за ущерб от загрязнения бункерным топливом. 2001.

[19] Конвенция о международной гражданской авиации. Приложение 13. Расследование авиационных происшествий и инцидентов. Международные стандарты и рекомендуемая практика. Июль 2010 года.

присвоения ответственности в ИКТ-среде, а также оценку характера и масштабов последствий.

4.5. Общий контекст международного инцидента в сфере ИКТ определяется, прежде всего, количеством государств, затронутых инцидентом, и характером международных отношений между ними. Данное событие может являться результатом непредвиденных действий, вовлекающих различные структуры, в том числе и вооруженные формирования, одного или более государств, или, наоборот, являться одним из многих преднамеренных, но незначительных провокаций, осуществляемых агентами одного государства против другого государства.

В последнем случае инцидент может иметь более серьезное значение.

4.6. Оценка характера и масштабов последствий инцидента, а также присвоение ответственности за инцидент в сфере ИКТ имеет целью определение субъекта международного права, к которому можно применить международно-правовую ответственность в связи с инцидентом.

Международно-правовая ответственность государства - это юридические последствия, которые могут наступить для субъекта международного права в результате его действий или бездействия, если при этом нарушены применимые к данному правоотношению международно-правовые нормы.

В качестве таких последствий предусматривается обязанность субъекта международного права ликвидировать вред, причинённый им другому субъекту международного права в результате нарушения международно-правового обязательства, или обязанность возместить материальный ущерб, причинённый в результате действий, не нарушающих нормы международного права, если такое возмещение предусматривается специальным международным договором.

4.7. Нормы и принципы международно-правовой ответственности государств, в том числе в сфере ИКТ, носят в основном характер международно-правового обычая, хотя некоторые из них подтверждены в договорных нормах. Деяние государства может быть квалифицировано как международно-противоправное лишь на основании международного права. Нарушение государством международного обязательства налицо в том случае, когда поведение или деяние этого государства не соответствуют тому, что требует от него указанное обязательство, вне зависимости от того, носит ли оно обычный или договорный характер. Реализация ответственности основывается на нормах обычного и договорного права[20].

[20] Ответственность государств за международно-противоправные деяния. Доклад 6 комитета Генеральной Ассамблеи ООН. Московская международная модель ООН 2012. М., 2011. С. 6.

4.8. Учитывая, что международные отношения в области инцидентов в сфере ИКТ в настоящее время не регулируются международными договорами, основным и, по существу, единственным источником права международной ответственности в рассматриваемом случае служит международный обычай, однако его применение сопряжено со сложностями, обусловленными особенностями ИКТ-среды (см. п. 1.7).

4.9. Проблема присвоения ответственности государству в связи с инцидентом в сфере ИКТ заключается в квалификации деяний органов, агентов, представителей государства и иных лиц и образований в качестве деяния государства. По общему правилу присвоения государство отвечает за деяния всех своих органов и должностных лиц. При этом государству не может быть присвоена международно-правовая ответственность за действия частных лиц, но ему может быть присвоена международно-правовая ответственность за свои действия в связи с действиями частных лиц.

В силу особенностей ИКТ-среды, изложенных выше (п. 1.7), проблемы атрибуции субъектов инцидента в сфере ИКТ и присвоения государству международно-правовой ответственности за инцидент в сфере ИКТ являются весьма сложными.

Методология решения проблемы атрибуции может базироваться на одном из двух оснований:

- презумпция доверия пострадавшего государства своим правоохранительным и специальным органам, занимавшимся исследованием инцидента и пришедшим к определенным заключениям, которые вряд ли можно считать объективными;
- презумпция доверия третьей стороне, которая не вовлечена в инцидент и в силу полномочий или обстоятельств может провести объективное расследование инцидента.

Методология решения проблемы присвоения государству международно-правой ответственности может опираться на весь спектр способов мирного разрешения международных споров: переговоры, обследования, посредничество, примирение, арбитраж, судебное разбирательство, обращение к региональным органам или соглашениям, или иные мирные средства.

4.10. Проблемы исследования инцидентов в сфере ИКТ осложняются также следующими обстоятельствами, указанными в п. 7 Доклада:

«7. Многообразие злонамеренных негосударственных субъектов (включая преступные группировки и террористов), их 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».

Фактически формируется международный рынок услуг осуществления деструктивной деятельности в ИКТ-среде, и поэтому в общем контексте события (инцидента) могут участвовать не только реальные исполнители, которых можно теоретически установить в процессе атрибуции, но и «заказчики».

Совместные меры государств, направленные на снижение опасности проявления указанных угроз, могут включать:

- политические решения государств по повышению координации деятельности правоохранительных органов и специальных служб в деле выявления физических лиц, групп или организаций, предлагающих услуги осуществления деструктивной деятельности в ИКТ-среде;
- подготовка и принятие международных договоров по криминализации деятельности лиц и организаций по созданию и распространению ИКТ, предназначенных для осуществления деструктивной деятельности в ИКТ-среде.

4.11. **Цель международного правового регулирования** заключается в снижении опасности возникновения международного спора или конфликта вокруг инцидентов в сфере ИКТ. Такие споры и конфликты возникают в случаях бездоказательного «назначения» государства виновным в инциденте и возложения на него обязанности исследовать весь контекст события.

По существу, речь идет о разработке и реализации определенных международных процессуальных норм, регулирующих правоприменительную деятельность субъектов международного права в сфере ИКТ.

4.12. Такие процессуальные нормы могут, например, включать:

- изучение международных обязательств государств в области предотвращения инцидентов, степени выполнения этих обязательств и определение условий и гарантий добросовестного исполнения обязательств, в том числе в области использования информации, получаемой в процессе выполнения оперативно-следственных мероприятий;
- установление правового режима компьютерных данных, представляющих интерес для целей расследования;
- определение порядка предоставления компьютерных данных, представляющих интерес для расследования, лицам, уполномоченным проводить расследование по международному инциденту в сфере ИКТ;

- определение порядка предоставления необходимых для проведения расследования персональных данных, находящихся у операторов связи или провайдеров услуг сети Интернет;

- определение порядка поиска и изъятия компьютерных данных компетентными органами по делу о расследовании международного инцидента в сфере ИКТ;

- организация сбора данных о трафике в режиме реального времени;

- организация перехвата данных в сетях.

5. Подпункт c) «государства не должны заведомо позволять использовать их территорию для совершения международно-противоправных деяний с использованием ИКТ»

Комментарий к подпункту c) п.13

5.1. **Объектом международного правового регулирования** являются международные отношения по поводу использования государством своей территории.

5.2. **Предметом международного правового регулирования** являются международные отношения по поводу совершения с территории государства международно-противоправных деяний с использованием ИКТ.

5.3. **Цель международного правового регулирования** заключается в добровольном принятии государствами обязательств не позволять использовать их территорию для совершения заведомо международно-противоправных деяний с использованием ИКТ.

5.4. Международно-противоправное деяние представляет собой действие или бездействие государства, которое:

- присваивается государству по международному праву;

- представляет собой нарушение международно-правового обязательства данного государства.

В универсальных международных договорах отсутствуют признаки международно-правовых деяний с использованием ИКТ.

5.5. Полномочия государства по использованию его территории охватываются государственным суверенитетом – присущим государству верховенством на своей территории и его независимостью в сфере международных отношений. Предоставление государственной территории другим государствам или негосударственным образованиям для любых целей входит в область суверенных решений государства.

Как применить эти принципы международного права к использованию

ИКТ с территории государства, в настоящее время неясно. Здесь остается много нерешенных вопросов, которые составляют так называемую проблему «суверенитета в киберпространстве» или «цифрового суверенитета». К таким вопросам относятся, в частности, следующие:

- являются ли цифровые адреса объектов киберпространства частью государственной территории и каким образом на них распространяется верховенство государства;
- где заканчиваются пространственные пределы суверенитета государства в ИКТ-среде и каким международным договором (договорами) они закрепляются.

5.6. Идентификация объектов ИКТ-среды в процессе информационного обмена осуществляется не по территориальному адресу его расположения, регистрируемому органами государственной власти, а по цифровому адресу, выдаваемому американской неправительственной организацией Internet Corporation for Assigned Names and Numbers (ICAAN), которая осуществляет деятельность по поддержанию и развитию системы распределения и использования цифрового адресного пространства. Универсальный международный договор, который мог бы быть источником права в области международного правового регулирования отношений в области системы цифровой адресации, отсутствует.

По существу, правовое регулирование в данном случае осуществляется на основе международного обычая как проявление всеобщей практики, признанной в качестве правовой нормы. В соответствии с этим обычаем ICAAN обеспечивает создание и поддержание в актуальном состоянии глобальной системы цифровых адресов субъектов и объектов киберпространства. При этом организация ICANN не является международной межправительственной организацией и, следовательно, не является субъектом международного права и не обладает ни международной правоспособностью, ни дееспособностью, ни деликтоспособностью.

В связи с этим можно констатировать отсутствие в системе международных отношений субъекта, несущего международную ответственность за поддержание стабильности и обеспечение безопасности функционирования системы цифровой адресации, а также за устойчивость киберпространства.

5.7. При исследовании фактов использования территории государства для совершения международно-противоправных деяний с использованием ИКТ необходимо учитывать, что как субъективные, так и объективные составляющие этих фактов могут носить виртуальный характер. В связи с этим объективное исследование таких фактов возможно только на основе разработанной системы процессуальных норм, закреплённых

международным договором. Более подробно проблема присвоения ответственности государству в сфере ИКТ проанализирована выше (раздел 4).

5.8. Трактовка рассматриваемого правила в категориях международного права невозможна, поскольку в международном праве отсутствуют такие понятия, как «суверенитет в киберпространстве» и «международно-правовое деяние с использованием ИКТ» Для реализации и контроля выполнения этого правила необходимо предварительно решить задачи, указанные в п.п. 1.2, 1.7, 5.4, 5.5, 5.6, 5.7.

6. Подпункт d) «государства должны рассмотреть вопрос о наилучших путях сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, а также осуществлять другие совместные меры по противодействию таким угрозам. Государствам, возможно, потребуется рассмотреть вопрос о разработке новых мер в этой сфере»

Комментарий к подпункту d) п.13

6.1. **Объектом международного правового регулирования** являются международные процессуальные отношения в области сотрудничества государств в борьбе с террористическим и преступным использованием ИКТ.

6.2. **Предметом международного правового регулирования** является активизация сотрудничества государств в борьбе с террористическим и преступным использованием ИКТ.

6.3. **Цель международного правового регулирования** заключается в принятии государствами на себя добровольных обязательств:

- рассмотреть вопрос о наилучших путях сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ;
- осуществлять другие совместные меры по противодействию угрозам терроризма и преступности в сфере ИКТ;
- рассмотреть вопрос о целесообразности разработки новых мер в этой сфере.

6.4. Основой для развития сотрудничества государств в рассматриваемой области является резолюция Генеральной Ассамблеи ООН

(2001)[21], в которой отмечалась необходимость активизации усилий, направленных на более эффективную борьбу с преступлениями, связанными с применением компьютеров.

В частности, признавалась важность следующих мер:

- сотрудничество правоохранительных органов в расследовании случаев трансграничного преступного использования информационных технологий и судебном преследовании в этой связи должно координироваться всеми соответствующими государствами;
- обмен государствами информацией о проблемах, с которыми они сталкиваются в борьбе с преступным использованием информационных технологий;
- совершенствование режимов взаимной помощи для обеспечения своевременного расследования случаев преступного использования информационных технологий и своевременного сбора доказательств, а также обмена ими;
- совершенствование технологической среды создания информационных технологий для содействия предупреждению и обнаружению случаев преступного использования, отслеживанию преступников и сбору доказательств.

6.5. Вместе с тем, существующие механизмы международного сотрудничества не в полной мере способствуют полному и быстрому получению из другого государства доказательств в форме компьютерной информации[22] и поэтому необходимо разработать новые механизмы, которые позволят решить, в частности, следующие проблемы.

Традиционные формы сотрудничества государств в области правовой помощи по уголовным делам предусматривают направление письменных ходатайств (просьб) об оказании правовой помощи. Это требует относительно длительного времени для их пересылки, отработки и получения ответов, а как отмечалось выше (п. 1.7), в ИКТ-среде доказательственная информация (юридические факты) может быть быстро утрачена.

Даже быстро предпринимаемые в рамках взаимной правовой помощи меры в лучшем случае позволят обнаружить, закрепить и изъять лишь информационные следы, находящиеся на серверах, расположенных на территории определенного государства (например, страны местонахождения потерпевшего или страны пребывания лица, совершившего компьютерное

---

[21] Резолюция ГА ООН A/RES/55/63 от 22 января 2001 года «Борьба с преступным использованием информационных технологий».

[22] Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., Юрлитинформ, 2002.

преступление). Когда же компьютерное сообщение по телекоммуникационным каналам проходит через третью (четвертую, пятую) страну, оказание правовой помощи может длиться очень долго. Чем больше стран, через которые посылается сообщение, тем выше вероятность того, что правоохранительным органам не удастся с использованием традиционных форм сотрудничества отследить всю цепочку реализации преступления с использованием ИКТ.

В настоящее время криминализация деяний, которые можно считать террористическим и преступным использованием ИКТ, в различных странах различна, а универсального международного договора в этой области нет. В связи с этим сотрудничество государств зачастую тормозится принципом «двойного определения состава преступления», в соответствии с которым государство не может сотрудничать с другим в расследовании и судебном преследовании деяний, не криминализованных в запрашиваемом государстве. Создавшейся ситуацией пользуются и субъекты, планирующие и осуществляющие террористическое и преступное использование ИКТ: в цепочку включается так называемая «тихая гавань» - государство, в котором планируемое деяние не криминализовано.

7. Подпункт e) «в процессе обеспечения безопасного использования ИКТ государства должны соблюдать положения резолюций 20/8 и 26/13 Совета по правам человека о поощрении, защите и осуществлении прав человека в Интернете и резолюций 68/167 и 69/166 Генеральной Ассамблеи о праве на неприкосновенность личной жизни в эпоху цифровых технологий, чтобы обеспечить всестороннее уважение прав человека, включая право свободно выражать свое мнение»

Комментарий к подпункту e) п.13

7.1. **Объектом международного правового регулирования** являются международные отношения в области всестороннего уважения прав человека в процессе обеспечения безопасного использования ИКТ.

7.2. **Предметом международного правового регулирования** являются международные отношения по поводу соблюдения государствами положений резолюций 20/8 и 26/13 Совета по правам человека о поощрении, защите и осуществлении прав человека в Интернете и резолюций 68/167 и 69/166 Генеральной Ассамблеи о праве на неприкосновенность личной жизни в эпоху цифровых технологий.

7.3. **Цель международного правового регулирования** заключается в распространении международных обязательств государства в области всестороннего уважения прав человека на область обеспечения безопасного использования ИКТ.

7.4. Дилемма, которая стоит перед государством при выполнении рассматриваемого правила, состоит в том, что эти права не могут быть безграничными и безусловными, как заявлено в Международном пакте о гражданских и политических правах. В Статье 19 пакта говорится, что человек имеет право «искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения, или иными способами по своему выбору». При этом далее уточняется, что такое право налагает «особые обязанности и особую ответственность» и может быть ограничено в соответствии с законом:

«a) для уважения прав и репутации других лиц;

b) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения»[23]. Каждое государство должно находить разумный баланс между соблюдением прав человека и обеспечением безопасного использования ИКТ.

Сложности нахождения разумного баланса связаны также с тем, что, как отмечалось в п. 1.5, «в киберпространстве как конструктивная, так и деструктивная (враждебная, агрессивная, противоправная, террористическая) деятельность осуществляются с помощью одних и тех же технологий, на основе которых разрабатываются необходимые средства и инструменты». Кроме того, как отмечалось в п. 1.7, «анонимность Интернета… позволяет субъекту затруднить юридически значимую идентификацию его личности и установление ее отношения к тому или иному государству».

7.5. Обязательства государства по уважению прав человека связаны, прежде всего, с уважением права на свободу мысли, свободы выражения мнений, права на неприкосновенность частной жизни, а также с осуществлением борьбы с пропагандой войны, национальной, расовой или религиозной ненависти, представляющих собой подстрекательство к дискриминации, вражде или насилию[24].

7.6. Одной из граней указанного выше разумного баланса является так называемая проблема «фильтрации контента». Имеет ли право государство,

---

[23] Международный пакт о гражданских и политических правах. Принят резолюцией 2200 A (XXI) Генеральной Ассамблеи от 16 декабря 1966 года. Ст. 19.

[24] Международный пакт о гражданских и политических правах. Принят резолюцией 2200 A (XXI) Генеральной Ассамблеи от 16 декабря 1966 года. Ст. 20.

ссылаясь на необходимость обеспечения безопасности, фильтровать вредоносный контент в Интернете и блокировать Интернет-сайты с вредоносным содержанием?

События последних лет дали ответ на этот вопрос. Дело в том, что специально подготовленный контент «под маской» свободы выражения мнений, помноженный на практически неограниченные возможности комментирования и тиражирования контента средствами Интернета, превратился в эффективное информационное оружие для достижения террористических и политических целей (пропаганда идеологии терроризма, вовлечение в террористические организации новых сторонников, вмешательство во внутренние дела суверенных государств и т.д.).

7.7. При реализации рассматриваемого правила возникает такая же проблема, которая указывалась в п. 6.5 – различия в законодательствах различных государств по вопросам размещения в Интернет-сайтах вредоносной информации. Поэтому при блокировании таких сайтов в одном государстве они возникают в «тихой гавани» - государстве, в котором такая информация не признается вредоносной.

8. Подпункт f) «государство не должно осуществлять или заведомо поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит его обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения»

Комментарий к подпункту f) п.13

8.1. **Объектом международного правового регулирования** являются международные отношения по поводу деятельности государств в сфере ИКТ.

8.2. **Предметом международного правового регулирования** являются международные отношения по поводу некоторых ограничений на деятельность государств в сфере ИКТ.

8.3. **Цель международного правового регулирования** заключается в добровольном принятии государствами обязательств не осуществлять или не поддерживать деятельность в сфере ИКТ, если такая деятельность заведомо:

- противоречит обязательствам государства по международному праву;
- наносит преднамеренный ущерб критически важной инфраструктуре;

- иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения.

8.4. Трактовка рассматриваемого правила в категориях международного права невозможна, поскольку в международном праве отсутствуют такие понятия, как «сфера ИКТ», «деятельность в сфере ИКТ», «критически важная инфраструктура». Для реализации и контроля выполнения этого правила необходимо предварительно решить задачи, указанные в п.п. 1.2, 1.7.

9. Подпункт g) «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»

Комментарий к подпункту g) п.13

9.1. **Объектом международного правового регулирования** являются международные отношения в области обеспечения безопасности критически важной инфраструктуры. Данные вопросы относятся к суверенитету государства.

9.2. **Предметом международного правового регулирования** является противодействие угрозам в сфере ИКТ для обеспечения безопасности критически важной инфраструктуры.

9.3. **Цель международного правового регулирования** состоит в том, чтобы государства при обеспечении безопасности критически важных инфраструктур принимали во внимание резолюцию 58/199 Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции.

9.4. Необходимость выполнения государствами рассматриваемого правила обусловлена в частности, следующим:

- государства несут главную ответственность за обеспечение безопасности своих граждан от угроз в ИКТ-среде и, в частности, за обеспечение безопасности своей критически важной инфраструктуры;
- эффективность деятельности государства по обеспечению безопасности своей критически важной инфраструктуры можно существенно повысить, используя накопленный международный опыт, сосредоточенный, в частности, в резолюции 58/199 Генеральной

Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и других соответствующих резолюциях.

10. Подпункт h) «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»

Комментарий к подпункту h) п.13

10.1. **Объектом международного правового регулирования** являются международные отношения в области сотрудничества государств при обеспечении безопасности критически важной инфраструктуры.

10.2. **Предметом международного правового регулирования** являются международные отношения по поводу оказания помощи государствам, критически важная инфраструктура которых стала объектом злонамеренных действий в сфере ИКТ.

10.3. **Цель международного правового регулирования** заключается в добровольном принятии государствами обязательств по оказанию помощи другим государствам (по их просьбе), критически важная инфраструктура которых стала объектом злонамеренных действий в сфере ИКТ и пострадала вследствие осуществления таких действий.

10.4. В рассматриваемом правиле государствам предлагается в добровольном порядке взять на себя обязательства по оказанию на основе международного сотрудничества помощи другим государствам в новой разновидности чрезвычайных ситуаций – в чрезвычайных ситуациях, возникающих вследствие злонамеренных действий в сфере ИКТ против критически важной инфраструктуры.

В соответствии с международным правом каждое государство в первую очередь несет ответственность за оказание помощи жертвам стихийных бедствий, случившихся на его территории, и поэтому пострадавшее

государство должно играть главную роль «в инициировании, организации, координации и оказании гуманитарной помощи на своей территории» [25].

В соответствии с принципом суверенного равенства государств международная помощь оказывается, прежде всего, на основе заключенных международных договоров и в определенных этими договорами порядке и случаях.

10.5. Порядок оказания международной помощи в случае некоторых разновидностей чрезвычайных ситуаций закреплен в соответствующих универсальных международных договорах[26] [27]. В случае чрезвычайных ситуаций, возникающих вследствие злонамеренных действий в сфере ИКТ против критически важной инфраструктуры, можно действовать аналогично. Вместе с тем целесообразно в рамках выполнения *правила а)* (см. раздел 3) разработать универсальный международный договор об оказании помощи в чрезвычайных ситуациях, возникающих вследствие злонамеренных действий в сфере ИКТ против критически важной инфраструктуры.

11. Подпункт i) «государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование пагубных скрытых функций»

Комментарий к подпункту i) п.13

11.1. **Объектом международного правового регулирования** являются международные отношения по поводу безопасности продуктов ИКТ.

11.2. **Предметом международного правового регулирования** являются международные отношения по поводу обеспечения целостности каналов поставки продуктов ИКТ конечному пользователю, а также предупреждения распространения злонамеренных программных и

[25] Резолюция Генеральной Ассамблеи ООН 57/150 от 16 декабря 2002 «Повышение эффективности и укрепление координации международной помощи при проведении поисково-спасательных операций в городах».

[26] Конвенция о помощи в случае ядерной или радиационной аварийной ситуации. Принята Генеральной конференцией Международного агентства по атомной энергии на ее специальной сессии 26 сентября 1986 года.

[27] Конвенция Тампере о предоставлении телекоммуникационных ресурсов для смягчения последствий бедствий и осуществления операций по оказанию помощи. Принята 18 июня 1998 года.

технических средств в сфере ИКТ и использования пагубных скрытых функций.

11.3. Проблема безопасности продуктов ИКТ – одна из центральных на пути к созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Именно в продуктах ИКТ заложены те факторы уязвимости, о которых говорится в *правиле j)* и на которых построена деструктивная (враждебная, агрессивная, противоправная, террористическая) деятельность в киберпространстве. Противодействию такой деятельности, а значит и использованию злонамеренных программных и технических средств в сфере ИКТ и пагубных скрытых функций посвящены *правила a), b), c), f), g), h).* Поэтому для решения проблемы безопасности продуктов ИКТ необходимо задействовать все механизмы, предусмотренные и/или запланированные для разработки в указанных правилах.

Необходимость решения проблемы целостности каналов поставки продуктов ИКТ отмечалась и в предыдущих Докладах Группы (2010, 2013 гг.):

- система поставок ИКТ может подвергнуться злонамеренному воздействию или быть нарушена таким образом, что это скажется на обычном, безопасном и надежном использовании ИКТ;
- включение в ИКТ вредоносных скрытых функций может подорвать доверие к товарам и услугам, вызвать недоверие к торговле и сказаться на национальной безопасности;
- возможность создания и широкомасштабного применения государствами или негосударственными субъектами сложных вредоносных инструментов и средств повышает риск ошибочной идентификации и непреднамеренной эскалации инцидентов в сфере ИКТ;
- возможность включения в ИКТ скрытых вредоносных функций, которые могут использоваться для подрыва безопасности и надежности использования ИКТ и всей системы производства и сбыта информационных товаров и информационно-технических услуг, а также для подрыва доверия между контрагентами в сфере торговли и причинения ущерба национальной безопасности.

Предложенные в *правиле i)* добровольные и необязательные разумные меры возлагают всю тяжесть решения рассматриваемой проблемы на государство - потребителя продуктов ИКТ. При этом не включаются ни государства, организации которых производят продукты ИКТ, ни механизмы международного сотрудничества, ни механизмы частно-государственного партнерства. Тем самым можно констатировать, что содержание *правила i)* не соответствует масштабу рассматриваемой проблемы.

11.4. В соответствии с изложенным в п. 11.3, **целью международного**

правового регулирования, адекватной объекту (см. п. 11.1) и предмету (см. п.11.2), должна быть разработка международного механизма регулирования, производства и поставки на международный рынок продуктов ИКТ с учетом требований безопасности.

На пути достижения этой цели необходимо учесть и следующие обстоятельства.

Корпоративные правила поставки продуктов ИКТ на мировой рынок, а также организации сопровождения (обновления) этих продуктов на этапах их эксплуатации не содержат механизмов национального и международного контроля безопасности поставляемых и эксплуатируемых продуктов. Данное обстоятельство ограничивает возможности государства-потребителя продуктов ИКТ по обеспечению безопасности использования этих продуктов.

Отсутствуют международные договоры, регулирующие вопросы международного сотрудничества в области обеспечения безопасности использования программного обеспечения со свободными лицензиями и безопасности репозиториев с таким программным обеспечением, которое активно используется многими организациями-производителями продуктов ИКТ.

В качестве примера приведем российское определение понятия «техническое регулирование»:

- правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, а также в области установления и применения на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг и правовое регулирование отношений в области оценки соответствия[28].

12. Подпункт j) «государства должны способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможности и устранить возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры»

Комментарий к подпункту j) п.13

[28] Федеральный закон от 27 декабря 2002 года, № 184-ФЗ «О техническом регулировании».

12.1. **Объектом международного правового регулирования** являются международные отношения в области международного сотрудничества по вопросам обеспечения безопасности в сфере ИКТ.

12.2. **Предметом международного правового регулирования** являются международные отношения по поводу обмена информацией между государствами о факторах уязвимости в сфере ИКТ и методах борьбы с этими факторами.

12.3. **Цель международного правового регулирования** заключается в повышении безопасности глобальной ИКТ-среды за счет выравнивания компетенций различных государств в области факторов уязвимости в сфере ИКТ и методов борьбы с этими факторами.

Актуальность предлагаемого правила объясняется тем, что в силу глобальности ИКТ-среды ее безопасность определяется безопасностью самого слабого звена, в частности, государства, не обладающего необходимой компетенцией в области факторов уязвимости в сфере ИКТ и методов борьбы с этими факторами.

13. Подпункт k) «государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным и 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»

Комментарий к подпункту k) п.13

13.1. **Объектом международного правового регулирования** являются международные отношения по поводу деятельности государств в сфере ИКТ.

13.2. **Предметом международного правового регулирования** являются международные отношения по поводу ограничений на деятельность государств в сфере ИКТ, которая могла бы затронуть нормальное функционирование уполномоченных групп экстренной готовности к компьютерным инцидентам (ГЭГКИ)[29],в том числе, нанести ущерб информационным системам ГЭГКИ.

[29] Community Emergency Response Team - CERT.

13.3. **Целью международного правового регулирования** является обеспечение (со стороны государств) нормального функционирования международной сети уполномоченных ГЭГКИ, которая является важной составляющей системы международной информационной безопасности.

13.4. Трактовка рассматриваемого правила в категориях международного права невозможна, поскольку в международном праве отсутствуют такие понятия, как «уполномоченные ГЭГКИ», «ущерб информационным системам». Для реализации и контроля выполнения этого правила необходимо предварительно решить задачи, указанные в п.п. 1.2, 1.7.