Организация Объединенных Наций A/75/816*

Генеральная Ассамблея

Distr.: General
18 March 2021
Russian
Original: English

Семьдесят пятая сессия
Пункт 98 повестки дня
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Записка Генерального секретаря

Генеральный секретарь имеет честь препроводить членам Генеральной Ассамблеи доклад Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, подготовленный во исполнение резолюции 73/27 и решения 75/550 Ассамблеи.

* Переиздано по техническим причинам 12 октября 2021 года.

21-03673* (R) 121021 121021

Доклад Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

I. Введение

1. В своей резолюции 73/27 Генеральная Ассамблея постановила созвать, начиная с 2019 года, рабочую группу открытого состава, действующую на основе консенсуса, в целях продолжения в качестве приоритета дальнейшей выработки норм, правил и принципов ответственного поведения государств и путей их реализации; при необходимости внесения в них изменений или формулирования дополнительных правил поведения; изучения возможности организации регулярного институционального диалога с широким кругом участников под эгидой Организации Объединенных Наций; а также продолжения в целях выработки общего понимания исследования существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению и того, как международное право применяется к использованию информационно-коммуникационных технологий государствами, а также мер укрепления доверия и наращивания потенциала и представления доклада о результатах данного исследования Ассамблее на ее семьдесят пятой сессии; и предусмотреть возможность проведения за счет добровольных взносов межсессионных консультационных встреч с заинтересованными сторонами, а именно бизнесом, неправительственными организациями и научным сообществом, для обмена взглядами по вопросам, входящим в мандат группы. Ассамблея постановила также, что рабочая группа должна провести свою организационную сессию в июне 2019 года для согласования организационных мер, связанных с рабочей группой.

2. В своем решении 75/550 Генеральная Ассамблея, отметив, что в связи с пандемией коронавирусного заболевания (COVID-19) третья и заключительная основная сессия, запланированная на 6–10 июля 2020 года, была отменена, постановила, что Рабочая группа открытого состава, продолжая свою работу в соответствии со своим мандатом согласно резолюции 73/27 Ассамблеи, созовет свою третью и заключительную основную сессию 8–12 марта 2021 года.

II. Организационные вопросы

A. Открытие и продолжительность сессий

3. Рабочая группа провела свою организационную сессию 3 июня 2019 года, свою первую основную сессию 9–13 сентября 2019 года, свою вторую основную сессию 10–14 февраля 2020 года и свою третью основную сессию 8–12 марта 2021 года в Центральных учреждениях.

4. Основную поддержку Рабочей группе оказывали Управление по вопросам разоружения и Институт Организации Объединенных Наций по исследованию проблем разоружения. Секретариатское обслуживание обеспечивал Департамент по делам Генеральной Ассамблеи и конференционному управлению.

B. Участники

5. Список участников основных сессий приводится в документах A/AC.290/2019/INF/1, A/AC.290/2020/INF/1 и A/AC.290/2021/INF/1.

C. Должностные лица

6. На своей организационной сессии 3 июня 2019 года Рабочая группа путем аккламации избрала Председателем Юэрга Лаубера (Швейцария).

D. Утверждение повестки дня

7. На той же сессии Рабочая группа утвердила повестку дня всех своих сессий, содержащуюся в документе A/AC.290/2019/1. Повестка дня включает следующие пункты:

1. Выборы должностных лиц.
2. Утверждение повестки дня.
3. Организация работы.
4. Общий обмен мнениями.
5. Обсуждение вопросов существа, указанных в пункте 5 резолюции 73/27 Генеральной Ассамблеи:
   a) продолжение дальнейшей выработки норм, правил и принципов ответственного поведения государств, перечисленных в пункте 1 резолюции 73/27 Генеральной Ассамблеи, и путей их реализации и при необходимости внесение в них изменений или формулирование дополнительных правил поведения;
   b) изучение возможности организации регулярного институционального диалога с широким кругом участников под эгидой Организации Объединенных Наций;
   c) продолжение в целях выработки общего понимания исследования существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению;
   d) как международное право применяется к использованию информационно-коммуникационных технологий государствами;
   e) меры укрепления доверия;
   f) наращивание потенциала и концепции, упомянутые в пункте 3 резолюции 73/27 Генеральной Ассамблеи.
6. Прочие вопросы.
7. Утверждение заключительного доклада.

8. Кроме того, на той же сессии Рабочая группа постановила проводить свою работу в соответствии с правилами процедуры главных комитетов Генеральной Ассамблеи, действуя при этом на основе консенсуса в соответствии с резолюцией 73/27 Ассамблеи. Группа постановила также, что в соответствии с

правилами процедуры и практикой Ассамблеи все государства-члены имеют право быть представленными в Группе. Государства, не являющиеся членами Организации Объединенных Наций, межправительственные организации и структуры, которым Ассамблея предоставила статус наблюдателя, получили постоянное приглашение участвовать в сессиях и работе Группы в качестве наблюдателей. Соответствующие подразделения системы Организации Объединенных Наций будут также приглашаться к участию исключительно в целях информационного технического сопровождения. Кроме того, соответствующие неправительственные организации, имеющие консультативный статус при Экономическом и Социальном Совете, согласно резолюции 1996/31 должны уведомлять секретариат Группы о своем желании принять участие в ее работе. Другие заинтересованные неправительственные организации, имеющие отношение к сфере деятельности и целям Группы и обладающие компетентностью в этой области, должны также сообщать секретариату Группы о своей заинтересованности, и, соответственно, им будет предложено принять участие в работе Группы в качестве наблюдателей на основе процедуры отсутствия возражений.

E. Организация работы

9. На первых заседаниях каждой из основных сессий, которые состоялись, соответственно, 9 сентября 2019 года, 10 февраля 2020 года и 8 марта 2021 года, Рабочая группа согласовывала порядок организации своей работы, содержащийся в документах A/AC.290/2019/2, A/AC.290/2020/1 и A/AC.290/2021/1.

F. Документация

10. С полным перечнем всех официальных документов, рабочих документов, технических документов и других документов, имеющихся в распоряжении Рабочей группы, можно ознакомиться на следующем специальном веб-сайте: www.un.org/disarmament/open-ended-working-group/.

G. Деятельность Рабочей группы

11. На своей первой основной сессии в ходе девяти пленарных заседаний Рабочая группа рассмотрела пункты 3–5 повестки дня.

12. На своей второй основной сессии в ходе девяти пленарных заседаний Рабочая группа продолжила рассмотрение пункта 5 повестки дня.

13. На своей третьей основной сессии Рабочая группа рассмотрела пункты 5–7 повестки дня.

14. С тем чтобы продолжить свою работу по время пандемии коронавирусного заболевания (COVID-19), Рабочая группа провела неофициальные виртуальные заседания 15, 17 и 19 июня и 2 июля 2020 года; 29 сентября — 1 октября 2020 года; 17–19 ноября 2020 года; 1–3 декабря 2020 года и 18, 19 и 22 февраля 2021 года.

15. В период со 2 по 4 декабря 2019 года Рабочая группа провела неофициальное межсессионное консультативное совещание с участием многих заинтересованных сторон. По просьбе Председателя Группы на этом совещании

председательствовал директор Агентства кибербезопасности Сингапура Дэвид Ко, и подготовленное им резюме работы было представлено и разослано членам Группы[1].

III. Утверждение доклада

16. На своей третьей основной сессии 12 марта 2021 года Рабочая группа рассмотрела пункт 7 повестки дня, озаглавленный «Утверждение доклада», и утвердила свой доклад, содержащийся в документе A/AC.290/2021/L.1 с внесенными в него устными исправлениями и в документе A/AC.290/2021/CRP.2.

17. Поскольку из-за ограничений, введенных в Центральных учреждениях Организации Объединенных Наций в связи с пандемией COVID-19, число заседаний Рабочей группы на ее третьей основной сессии было сокращено, подборка заявлений с разъяснением позиций будет издана в качестве документа A/AC.290/2021/INF.2.

[1] URL: www.un.org/disarmament/open-ended-working-group/.

Приложение I*

Заключительный содержательный доклад

A. Введение

1. Несмотря на то, что с момента создания Организации Объединенных Наций 75 лет назад в мире произошли радикальные преобразования, цель ее деятельности и ее идеалы, не утратившие своей актуальности, сохраняют свое основополагающее значение. Помимо подтверждения своей приверженности фундаментальным правам человека и содействию улучшению экономического и социального положения всех людей и созданию условий для установления справедливости и соблюдения международного права государства заявили о решимости объединить свои силы для поддержания международного мира и безопасности[2].

2. Развитие информационно-коммуникационных технологий (ИКТ) затрагивает все три основные направления деятельности Организации Объединенных Наций: мир и безопасность, права человека и устойчивое развитие. Способствуя общественным и экономическим преобразованиям и расширяя возможности для сотрудничества, ИКТ и глобальная связь играют роль катализатора прогресса и развития человека.

3. Сегодня как никогда очевидна насущная необходимость установления и поддержания международного мира, безопасности, сотрудничества и доверия в ИКТ-среде. Негативные тенденции в сфере цифровых технологий могут подорвать международную безопасность и стабильность, негативно сказаться на экономическом росте и устойчивом развитии и помешать полному осуществлению прав человека и основных свобод. Речь идет о все более широком применении ИКТ злонамеренным образом.

4. Текущий общемировой кризис в области здравоохранения наглядно показывает фундаментальные преимущества ИКТ и нашу зависимость от них, в том числе в плане предоставления жизненно важных государственных услуг, распространения важной информации по вопросам общественной безопасности, разработки новаторских решений для обеспечения бесперебойной деятельности, ускорения исследований и содействия обеспечению непрерывности образования и социальной сплоченности с помощью средств виртуализации. В нынешних условиях неопределенности государства, а также частный сектор, ученые и другие субъекты используют цифровые технологии, с тем чтобы поддерживать связь между отдельными лицами и целыми сообществами и оказывать им услуги здравоохранения. В то же время пандемия коронавирусного заболевания (COVID-19) наглядно показала риски и последствия вредоносной деятельности, направленной на использование факторов уязвимости в то время, когда общество переживает тяжкие испытания. Она также подчеркнула необходимость преодоления цифрового разрыва, повышения устойчивости всех сообществ и секторов к потрясениям и неизменного применения подхода, ориентированного на интересы людей.

5. Поскольку ИКТ могут использоваться в целях, несовместимых с задачами поддержания международного мира, стабильности и безопасности, Генеральная

* Публикуется без официального редактирования.

[2] Преамбула Устава Организации Объединенных Наций.

Ассамблея признала[3], что распространение и использование ИКТ затрагивают интересы всего мирового сообщества и что широкое международное взаимодействие способствует принятию наиболее действенных ответных мер.

6. В свете вышеизложенного создание Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (РГОС) согласно резолюции 73/27 Генеральной Ассамблеи дало возможность добиться подвижек в рассмотрении этого важнейшего вопроса. Группа предоставила всем государствам демократичную, транспарентную и инклюзивную площадку для выражения их мнений и расширения сотрудничества в вопросах, касающихся ИКТ в контексте международной безопасности. Активное участие государств — членов Организации Объединенных Наций и вовлеченность целого ряда других соответствующих заинтересованных сторон свидетельствуют об общем стремлении и коллективной заинтересованности международного сообщества создать мирную и безопасную для всех ИКТ-среду и об их решимости сотрудничать в достижении этой цели.

7. Создание РГОС стало важной вехой в процессе международного сотрудничества на пути к обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Для изучения существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению с 2003 года шесть раз создавались группы правительственных экспертов[4]. В трех принятых на основе консенсуса докладах (от 2010, 2013 и 2015 годов[5]), которые, по сути, имеют взаимодополняющий характер, эти группы рекомендовали 11 добровольных, не имеющих обязательной силы норм ответственного поведения государств и признали, что со временем могут быть разработаны дополнительные нормы. Кроме того, в них содержались рекомендации в отношении конкретных мер в области укрепления доверия, наращивания потенциала и сотрудничества. В них также было подтверждено, что международное право, в частности Устав Организации Объединенных Наций, применимо и необходимо для поддержания мира, безопасности и стабильности в ИКТ-среде. В резолюции 70/237 Генеральной Ассамблеи государства-члены приняли консенсусное решение при использовании ИКТ руководствоваться докладом группы правительственных экспертов 2015 года, тем самым закрепив первоначальные рамки ответственного поведения государств в области использования ИКТ. В этой связи РГОС приняла также к сведению резолюции 73/27 и 73/266 Генеральной Ассамблеи.

8. Опираясь на эти основополагающие принципы и подтверждая эти рамки, РГОС стремится найти точки соприкосновения и взаимопонимания между всеми государствами — членами Организации Объединенных Наций по вопросу общемировой значимости. Для изучения существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению РГОС в соответствии со своим мандатом рассмотрела вопросы, касающиеся дальнейшего развития норм, правил и принципов ответственного поведения государств, как международное право применяется к использованию ИКТ государствами, мер укрепления доверия, укрепления потенциала и возможности организации регулярного институционального диалога с широким кругом участников под эгидой Организации Объединенных Наций. В своих усилиях по достижению консенсуса и содействию международному миру, безопасности,

[3] См., например, шестой пункт преамбулы резолюции 53/70 Генеральной Ассамблеи.
[4] Резолюции 58/32, 60/45, 66/24, 68/243, 70/237 и 73/266 Генеральной Ассамблеи.
[5] A/65/201, A/68/98 и A/70/174.

сотрудничеству и доверию РГОС руководствовалась принципами инклюзивности и транспарентности.

9. Организации Объединенных Наций следует и далее играть ведущую роль в содействии диалогу по вопросам использования государствами ИКТ. РГОС учитывает важность и взаимодополняющий характер специализированных обсуждений аспектов цифровых технологий в рамках других органов и форумов Организации Объединенных Наций.

10. Главную ответственность за поддержание международного мира и безопасности несут государства, однако использовать ИКТ таким образом, чтобы не создавать угрозу миру и безопасности, обязаны все заинтересованные стороны. Поскольку аспекты международной безопасности ИКТ пересекаются со многими областями и дисциплинами, ценным подспорьем для РГОС оказались экспертная оценка, опыт и знания, которыми поделились представители межправительственных организаций, региональных организаций, гражданского общества, частного сектора, научных кругов и технического сообщества. Трехдневное неофициальное консультативное совещание РГОС, состоявшееся в декабре 2019 года, позволило провести плодотворное обсуждение с участием государств и широкого круга других заинтересованных сторон[6]. Кроме того, в письменных материалах и в ходе неофициальных консультаций с РГОС эти заинтересованные стороны представили конкретные предложения и примеры передовой практики. Некоторые делегации также провели по собственной инициативе консультации с участием многих заинтересованных сторон и подготовили по их итогам материалы для представления Рабочей группе открытого состава.

11. С учетом различий в условиях, возможностях и приоритетах государств и регионов РГОС признает, что распределение выгод, связанных с цифровыми технологиями, не является равномерным и что насущной задачей международного сообщества остается сокращение цифрового разрыва, в том числе за счет обеспечения всеобщего, инклюзивного и недискриминационного доступа к ИКТ и возможностей подключения к сети.

12. РГОС приветствует высокий уровень участия женщин-делегатов в работе ее сессий и то большое внимание, которое уделяется в ее обсуждениях гендерным аспектам. РГОС подчеркивает важность сокращения гендерного цифрового разрыва и содействия эффективному и значимому участию и лидерству женщин в процессах принятия решений, связанных с использованием ИКТ в контексте международной безопасности.

13. РГОС подчеркивает, что отдельные элементы ее мандата связаны между собой и взаимно подкрепляют друг друга и в своей совокупности способствуют созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

B. Выводы и рекомендации

14. Рассмотрев содержательные аспекты мандата РГОС и напомнив, что в резолюции 73/27 Генеральной Ассамблеи приветствовалась эффективная работа, выполненная в 2010, 2013 и 2015 годах Группой правительственных экспертов

[6] См. “Chair’s Summary of the Informal intersessional consultative meeting of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security”, URL: https://www.un.org/disarmament/open-ended-working-group/.

по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, и подготовленные в итоге соответствующие доклады, препровожденные Генеральным секретарем[7], государства пришли к следующим выводам и рекомендациям, которые включают конкретные действия и совместные меры по противодействию связанным с использованием ИКТ угрозам и содействию созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

Существующие и потенциальные угрозы

15. По общему признанию государств, все большее беспокойство вызывают последствия злонамеренного использования ИКТ для поддержания международного мира и безопасности и, следовательно, для прав человека и развития. В частности, была выражена обеспокоенность по поводу расширения возможностей ИКТ, которые могут быть использованы для подрыва международного мира и безопасности. Вредоносные происшествия в сфере ИКТ становятся все более частыми и изощренными и постоянно эволюционируют и видоизменяются. Расширение коммуникационных возможностей и зависимости от ИКТ в отсутствие сопутствующих мер по обеспечению безопасности ИКТ может породить непреднамеренные риски, сделав общество более уязвимым для злонамеренной деятельности в сфере ИКТ. Несмотря на неоценимую выгоду ИКТ для человечества, их злонамеренное использование может иметь значительные и далеко идущие негативные последствия.

16. Государства напомнили, что ряд государств занимается наращиванием потенциала в сфере ИКТ для военных целей. Они напомнили также, что применение ИКТ в будущих конфликтах между государствами становится все более вероятным. Продолжающееся увеличение числа инцидентов, связанных со злонамеренным использованием ИКТ государственными и негосударственными субъектами, включая террористов и преступные группировки, является тревожной тенденцией. Некоторые негосударственные субъекты демонстрируют, что они располагают такими возможностями использования ИКТ, которые ранее были доступны только государствам.

17. Государства также пришли к выводу о том, что любое использование ИКТ государствами таким образом, который противоречит их обязательствам в соответствие с рамками, включающим добровольные нормы, международное право и меры укрепления доверия, подрывает международный мир и безопасность, доверие и стабильность в отношениях между государствами и может повысить вероятность возникновения в будущем межгосударственных конфликтов.

18. Государства пришли к выводу о том, что вредоносная деятельность в сфере ИКТ может иметь разрушительные последствия для безопасности, а также разрушительные экономические, социальные и гуманитарные последствия для критически важной инфраструктуры и критически важной информационной инфраструктуры, обеспечивающей оказание основных услуг населению. Хотя определение того, какие объекты инфраструктуры считаются критически важными, является прерогативой каждого отдельного государства, к таким объектам инфраструктуры могут относиться медицинские учреждения, финансовые службы, объекты энергетики и водоснабжения, транспорт и санитарные объекты. Реальную и растущую озабоченность вызывают злонамеренные действия с использованием ИКТ, направленные против объектов критически важной

[7] A/65/201, A/68/98 и A/70/174.

инфраструктуры и объектов критически важной информационной инфраструктуры и подрывающие доверие к политическим и избирательным процессам и государственным институтам или оказывающие влияние на общедоступность и целостность Интернета. Такие объекты инфраструктуры могут находиться в собственности, под управлением или в эксплуатации частного сектора, предоставляться в пользование другому государству или быть частью сети с участием другого государства или совместно эксплуатироваться в разных государствах. Вследствие этого для поддержания их целостности, функционирования и доступности может потребоваться межгосударственное сотрудничество или сотрудничество государства и частного сектора.

19. Государства пришли также к выводу о том, что деятельность в сфере ИКТ, противоречащая обязательствам по международному праву и наносящая преднамеренный ущерб критически важной инфраструктуре или иным образом препятствующая использованию и функционированию критически важной инфраструктуры для обслуживания населения, может представлять угрозу не только безопасности, но и государственному суверенитету, а также экономическому развитию и источникам средств к существованию и, в конечном счете, безопасности и благополучию людей.

20. Поскольку все государства во все большей степени полагаются на цифровые технологии, государства пришли к выводу о том, что отсутствие осведомленности и надлежащих возможностей для выявления злонамеренных действий с использованием ИКТ, а также соответствующей защиты и реагирования, может сделать их более уязвимыми. Как наглядно показала нынешняя чрезвычайная ситуация в области здравоохранения в мире, во время кризиса действие существующих факторов уязвимости может многократно усилиться.

21. Государства пришли к выводу о том, что в зависимости от уровня цифровизации, имеющихся возможностей, а также безопасности и надежности ИКТ, наличия инфраструктуры и уровня развития ИКТ государства могут испытывать воздействие угроз по-разному. Кроме того, угрозы могут по-разному воздействовать на различные группы и различных субъектов, включая молодежь, пожилых людей, женщин и мужчин, уязвимые группы населения, представителей отдельных профессий, малые и средние предприятия и т. д.

22. Учитывая все более тревожную обстановку в плане цифровых угроз и принимая во внимание, что от этих угроз не защищено ни одно государство, государства особо подчеркнули, что необходимо в срочном порядке применять совместные меры по борьбе с такими угрозами и продолжать разработку таких мер. Было подтверждено, что взаимодействие при неограниченно широком участии, когда это практически возможно, может принести более эффективные и многообещающие результаты. В этой связи была также подчеркнута ценность дальнейшего укрепления сотрудничества – при необходимости с гражданским обществом, частным сектором, научными кругами и техническим сообществом.

23. Государства особо подчеркнули положительные экономические и социальные возможности, которые могут быть получены благодаря ИКТ, и отметили, что обеспокоенность вызывают не сами технологии, а их ненадлежащее использование.

Правила, нормы и принципы ответственного поведения государств

24. Добровольные, не имеющие обязательной силы нормы ответственного поведения государств могут уменьшить риски для международного мира,

безопасности и стабильности и могут играть важную роль в повышении предсказуемости и уменьшении риска неправильного восприятия, способствуя тем самым предотвращению конфликтов. Государства подчеркнули, что такие нормы отражают ожидания и стандарты международного сообщества в отношении поведения государств при использовании ими ИКТ и позволяют международному сообществу оценивать действия государств. Исходя из положений резолюции 70/237 Генеральной Ассамблеи и признавая положения резолюции 73/27 Генеральной Ассамблеи, к государствам был обращен призыв избегать и воздерживаться от таких видов применения ИКТ, которые не соответствуют нормам ответственного поведения государств.

25. Государства вновь подтвердили, что нормы не заменяют собой обязательства или права государств по международному праву, которые носят обязательный характер, и не изменяют их, а скорее содержат дополнительные конкретные указания в отношении того, что представляет собой ответственное поведение государств при использовании ИКТ. Нормы не направлены на ограничение или запрещение действий, которые не противоречат международному праву.

26. Согласившись с необходимостью защищать всю критически важную инфраструктуру и критически важную информационную инфраструктуру, обеспечивающую оказание основных услуг населению, а также стремясь обеспечить общедоступность и целостность Интернета, государства пришли также к выводу о том, что пандемия COVID-19 высветила важность защиты инфраструктуры систем здравоохранения, включая медицинские службы и объекты, посредством исполнения норм, касающихся объектов критически важной инфраструктуры, например, таких норм, которые были утверждены на основе консенсуса в резолюции 70/237 Генеральной Ассамблеи Организации Объединенных Наций.

27. Государства подтвердили, что важно поддерживать и продолжать усилия по осуществлению на глобальном, региональном и национальном уровнях норм, которыми соглашаются руководствоваться государства.

28. Подтверждая резолюцию 70/237 Генеральной Ассамблеи и признавая резолюцию 73/27 Генеральной Ассамблеи, государства должны принимать разумные меры для обеспечения целостности каналов поставки, в том числе посредством разработки объективных коллективных мер, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ; должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование скрытых вредоносных функций; и должны способствовать ответственному представлению информации об уязвимостях.

29. Государства вновь подтвердили, что, принимая во внимание уникальные особенности ИКТ и учитывая представленные в рамках РГОС предложения в отношении норм, разработку со временем дополнительных норм можно было бы продолжить. Государства также пришли к выводу о том, что дальнейшее развитие норм и применение существующих норм не являются взаимоисключающими, а могут происходить одновременно.

Рекомендации Рабочей группы открытого состава

30. Государствам следует добровольно анализировать национальные усилия по применению норм, накапливать опыт и передовую практику в части применения норм и обмениваться ими, а также продолжать информировать Генерального секретаря о своих национальных позициях и оценках в этой связи.

31. Государства не должны осуществлять и заведомо поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит их обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения. Кроме того, государствам следует продолжать укреплять меры по защите всей критически важной инфраструктуры от угроз, связанных с использованием ИКТ, и расширять обмен передовым опытом в области защиты критически важной инфраструктуры.

32. Государствам следует, действуя в партнерстве с соответствующими организациями, включая Организацию Объединенных Наций, продолжать содействовать реализации и разработке норм ответственного поведения всеми государствами. Государствам рекомендуется предоставлять экспертные и материальные ресурсы, если у них имеются такие возможности.

33. Ссылаясь на резолюцию 70/237 Генеральной Ассамблеи и признавая резолюцию 73/27 Генеральной Ассамблеи, государства принимают к сведению предложения, сделанные государствами относительно разработки правил, норм и принципов ответственного поведения государств в ходе будущих обсуждений в рамках Организации Объединенных Наций вопросов, касающихся ИКТ, учитывая, что резолюцией 75/240 Генеральной Ассамблеи была учреждена Рабочая группа открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025.

Международное право

34. Отмечая резолюцию 70/237 Генеральной Ассамблеи, а также признавая резолюцию 73/27 Генеральной Ассамблеи, согласно которой была учреждена РГОС, государства вновь подтвердили, что международное право, и, в частности, Устав Организации Объединенных Наций, применимо и имеет ключевое значение для поддержания мира и стабильности и содействия обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. В этой связи к государствам был обращен призыв избегать и воздерживаться от принятия каких бы то ни было мер, не соответствующих международному праву, в частности Уставу Организации Объединенных Наций. Государства пришли также к выводу о том, что необходимо продолжить работу над углублением общего понимания того, как международное право применяется к использованию ИКТ государствами.

35. Государства также подтвердили, что государствам следует стремиться урегулировать споры мирными средствами, такими, как переговоры, проведение расследований, посредничество, примирение, арбитраж, судебное разбирательство и обращение к региональным органам или договоренностям, либо иными мирными средствами на их усмотрение.

36. Государства пришли к выводу о том, что, с учетом уникальных особенностей ИКТ-среды, улучшения общего понимания применимости международного права к использованию ИКТ можно достичь благодаря обмену мнениями по этому вопросу между государствами и благодаря определению конкретных вопросов международного права для дальнейшего углубленного обсуждения в рамках Организации Объединенных Наций.

37. С тем чтобы улучшить понимание всеми государствами вопросов применимости международного права к использованию ИКТ государствами и

содействовать формированию консенсуса и общего понимания в международном сообществе, государства пришли к выводу о необходимости предпринять, руководствуясь соображениями непредвзятости и объективности, дополнительные усилия по созданию потенциала в области международного права, национального законодательства и политики.

Рекомендации Рабочей группы открытого состава

38. Государствам следует продолжать добровольно информировать Генерального секретаря о национальных взглядах и оценках в отношении применимости международного права к использованию ими ИКТ в контексте международной безопасности и продолжать на добровольной основе обмениваться такими национальными взглядами и практикой по другим соответствующим каналам.

39. Государствам, которые имеют такую возможность, следует продолжать, руководствуясь соображениями непредвзятости и объективности и действуя в соответствии с принципами, содержащимися в пункте 56 настоящего доклада, поддерживать дополнительные усилия по наращиванию потенциала в области международного права, национального законодательства и политики, с тем чтобы все государства могли способствовать достижению общего понимания того, как международное право применяется к использованию ИКТ государствами и содействовать достижению консенсуса в международном сообществе.

40. Государствам следует продолжать изучать и обсуждать в структуре будущих процессов в рамках Организации Объединенных Наций то, как международное право применяется к использованию ИКТ государствами, в качестве одного из важных шагов по уточнению и дальнейшему углублению общего понимания этого вопроса.

Меры укрепления доверия

41. Меры укрепления доверия, которые включают в себя меры обеспечения прозрачности, развития сотрудничества и повышения стабильности, могут способствовать предотвращению конфликтов, избегать случаев неправильного восприятия и недопонимания, а также могут использоваться для снижения напряженности. Они представляют собой одно из конкретных проявлений международного сотрудничества. При наличии необходимых ресурсов, возможностей и должного участия меры укрепления доверия могут способствовать укреплению общей безопасности, повышению устойчивости и использованию ИКТ в мирных целях. Кроме того, меры укрепления доверия могут способствовать практической реализации норм ответственного поведения государств, поскольку они способствуют укреплению доверия и повышению ясности, предсказуемости и стабильности в использовании ИКТ государствами. В сочетании с другими основополагающими элементами рамок ответственного поведения государств меры укрепления доверия могут также способствовать достижению общего понимания между государствами, способствуя тем самым созданию более мирной международной обстановки.

42. Поскольку меры укрепления доверия представляют собой добровольные обязательства, которые выполняются постепенно, они могут стать первым шагом к устранению между государствами недоверия, вытекающего из недопонимания, путем налаживания связей, наведения мостов и развития сотрудничества для достижения общей цели, представляющей взаимный интерес. Меры

укрепления доверия как таковые могут заложить основы для заключения расширенных, дополнительных договоренностей и соглашений в будущем.

43. Государства пришли к выводу о том, что диалог в рамках РГОС сам по себе является мерой укрепления доверия, поскольку он стимулирует открытый и прозрачный обмен мнениями относительно восприятия угроз и факторов уязвимости, ответственного поведения государств и других субъектов, а также передовой практики, способствуя в конечном счете коллективной разработке и применению рамок ответственного поведения государств при использовании ИКТ.

44. Кроме того, государства пришли к выводу о том, что Организация Объединенных Наций играет решающую роль в разработке и поддержке реализации мер укрепления доверия на общемировом уровне. В каждом из принятых консенсусом докладов групп правительственных экспертов содержались рекомендации в отношении практических мер укрепления доверия. В дополнение к этим конкретным рекомендациям по ИКТ Генеральная Ассамблея в принятой консенсусом резолюции 43/78 H одобрила Руководящие принципы для мер укрепления доверия, разработанные в рамках Комиссии Организации Объединенных Наций по разоружению, в которых изложены ценные принципы, цели и характеристики мер укрепления доверия, которые могут учитываться при разработке новых мер применительно к ИКТ.

45. Государства пришли к выводу о том, что региональные и субрегиональные организации, используя имеющееся у них в активе доверие и налаженные связи, прилагают значительные усилия для разработки мер укрепления доверия с учетом их конкретных условий и приоритетов, тем самым повышая осведомленность и способствуя распространению информации среди своих членов. Кроме того, региональные, межрегиональные и межорганизационные обмены могут способствовать созданию новых возможностей для сотрудничества, взаимодействия и взаимного обучения. Было отмечено, что, так как не все государства являются членами той или иной региональной организации и не все региональные организации разработали меры укрепления доверия, такие меры дополняют работу Организации Объединенных Наций и других организаций по продвижению мер укрепления доверия.

46. На основе обмена информацией об опыте и практике, который состоялся в рамках РГОС, государства пришли к выводу о том, что для обеспечения того, чтобы реализация мер укрепления доверия позволила достичь поставленных целей, необходимо существование уже функционирующих национальных и региональных механизмов и структур, а также создание адекватных ресурсов и возможностей, таких как национальные группы реагирования на компьютерные инциденты (CERTs).

47. Государства пришли к выводу о том, что такая конкретная мера, как создание национальных контактных пунктов, является не только самостоятельной мерой укрепления доверия, но и полезным средством для реализации многих других мер укрепления доверия и имеет неоценимое значение в условиях кризиса. Государства могут счесть целесообразным создание контактных пунктов, в частности, для координации по дипломатическим, политическим, правовым и техническим вопросам, а также для уведомления об инцидентах и реагирования на них.

Рекомендации Рабочей группы открытого состава

48. Государствам следует продолжать добровольно информировать Генерального секретаря о своих взглядах и оценках и представлять дополнительную информацию о полученном опыте и передовой практике в отношении соответствующих мер укрепления доверия на двустороннем, региональном или многостороннем уровне.

49. Государствам следует добровольно определять меры укрепления доверия и рассматривать возможность их принятия с учетом их конкретных обстоятельств, а также сотрудничать с другими государствами в реализации таких мер.

50. Государствам следует добровольно принимать меры обеспечения прозрачности посредством распространения соответствующей информации и сделанных выводов в подходящей форме и на соответствующих форумах, в том числе на портале по вопросам киберполитики Института Организации Объединенных Наций по исследованию проблем разоружения.

51. Государствам, которые еще не сделали этого, следует, учитывая различия в возможностях, рассмотреть вопрос о создании национальных контактных пунктов, в частности, на техническом, политическом и дипломатическом уровнях. Государствам следует также продолжать рассматривать способы создания реестра таких контактных пунктов на глобальном уровне.

52. Государствам следует изучить механизмы регулярного межрегионального обмена опытом и передовой практикой в области мер укрепления доверия, принимая во внимание различия в региональных условиях и структурах соответствующих организаций.

53. Государствам следует продолжать рассматривать меры укрепления доверия на двустороннем, региональном и многостороннем уровнях и способствовать созданию возможностей для совместной реализации мер укрепления доверия.

Наращивание потенциала

54. Способность международного сообщества предотвращать вредоносную деятельность в области ИКТ или смягчать ее последствия зависит от возможностей каждого государства в плане обеспечения готовности и реагирования. Это особенно важно для развивающихся государств и необходимо для того, чтобы содействовать их реальному участию в обсуждении вопросов ИКТ в контексте международной безопасности и обеспечить их способность устранять факторы уязвимости в критически важной инфраструктуре. Наращивание потенциала способствует развитию навыков, кадровых ресурсов, политики и институтов, повышающих устойчивость государств и их безопасность, с тем чтобы они могли в полной мере пользоваться благами цифровых технологий. Оно играет важную вспомогательную роль, выступая стимулом для соблюдения норм международного права и реализации норм ответственного поведения государств, а также для поддержки выполнения мер укрепления доверия. В мире, где существует цифровая взаимозависимость, выгоды от наращивания потенциала не ограничиваются первоначальными получателями, а способствуют созданию более безопасной и стабильной ИКТ-среды для всех.

55. Обеспечение открытой, безопасной, стабильной, доступной и мирной ИКТ-среды требует эффективного сотрудничества между государствами в целях снижения рисков для международного мира и безопасности. Наращивание

потенциала является важным аспектом такого сотрудничества и осуществляется в добровольном порядке как донорами, так и получателями.

56. Принимая во внимание широко признанные принципы и необходимость их дальнейшей проработки, государства пришли к выводу, что деятельность по наращиванию потенциала в области использования ИКТ государствами в контексте международной безопасности должна осуществляться на основе перечисленных ниже принципов.

Процесс и цель

- Процесс наращивания потенциала должен носить устойчивый характер и включать в себя конкретные мероприятия, проводимые различными субъектами и в интересах этих субъектов.
- Конкретные мероприятия должны иметь четкую цель и ориентированность на результат, способствуя при этом достижению общей цели создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.
- Деятельность по наращиванию потенциала должна быть основанной на фактах, нейтральной в политическом плане, прозрачной, подотчетной и носить безусловный характер.
- Деятельность по наращиванию потенциала должна осуществляться при полном соблюдении принципа государственного суверенитета.
- Может возникнуть необходимость в облегчении доступа к соответствующим технологиям.

Партнерские отношения

- Деятельность по наращиванию потенциала должна быть основана на взаимном доверии, определяться спросом, соответствовать определяемым государствами потребностям и приоритетам и должна осуществляться при полном признании принципа национальной ответственности за процесс. Участие партнеров в деятельности по наращиванию потенциала носит добровольный характер.
- Поскольку деятельность по наращиванию потенциала должна осуществляться с учетом конкретных потребностей и условий, все стороны являются активными партнерами, несущими общую, но дифференцированную ответственность, в том числе в отношении сотрудничества в разработке, осуществлении и мониторинге и оценке мероприятий по наращиванию потенциала.
- Все партнеры обязаны обеспечивать и соблюдать конфиденциальный характер национальной политики и планов.

Люди

- В основе деятельности по наращиванию потенциала, которая должна носить всеохватный, универсальный и недискриминационный характер, должны лежать уважение прав человека и основных свобод и учет гендерных аспектов.
- Должна обеспечиваться конфиденциальность чувствительной информации.

57. Государства пришли к выводу, что деятельность по наращиванию потенциала представляет собой взаимонаправленный процесс, своего рода улицу с двусторонним движением, где участники учатся друг у друга, а все стороны извлекают пользу из общего улучшения положения дел с безопасностью в сфере ИКТ во всем мире. Была также упомянута ценность сотрудничества Юг — Юг, Юг — Север, трехстороннего сотрудничества и сотрудничества региональной направленности.

58. Государства пришли к выводу о том, что наращивание потенциала должно способствовать превращению «цифровой пропасти» в цифровые возможности. В частности, наращивание потенциала должно быть ориентировано на содействие реальному участию развивающихся стран в соответствующих дискуссиях и форумах и на повышение устойчивости развивающихся стран в ИКТ-среде.

59. Государства пришли к выводу о том, что наращивание потенциала может способствовать пониманию и устранению системных и других рисков, обусловленных отсутствием безопасности в сфере ИКТ, недостаточно тесной увязкой технических и директивных возможностей на национальном уровне и сопутствующими проблемами неравенства и цифрового разрыва. Было признано, что особо важное значение имеет деятельность по наращиванию потенциала, которая позволяет государствам выявлять и защищать объекты национальной критически важной инфраструктуры и обеспечивать совместную защиту критически важной информационной инфраструктуры. Наращивание потенциала может также помочь государствам углубить понимание по вопросу о том, как применяется международное право. Повышению эффективности деятельности по наращиванию потенциала, приданию ей более стратегического характера и более тесной ее увязке с национальными приоритетами могут способствовать обмен информацией и координация на национальном, региональном и международном уровнях.

60. Государства пришли к выводу о том, что в дополнение к техническим навыкам, институциональному строительству и механизмам сотрудничества крайне необходимо накапливать экспертные знания в целом ряде областей дипломатии, права, политики, законодательства и нормативного регулирования. В этой связи была подчеркнута важность укрепления дипломатического потенциала для участия в международных и межправительственных процессах.

61. Государства напомнили о том, что в отношении наращивания потенциала необходимо применять конкретный и практико-ориентированный подход. Государства пришли к выводу о том, что конкретные меры могли бы предусматривать поддержку как на политическом, так и на техническом уровнях, такую как разработка национальных стратегий кибербезопасности, предоставление доступа к соответствующим технологиям, оказание поддержки группам реагирования на компьютерные инциденты или группам реагирования на инциденты в сфере компьютерной безопасности, а также разработка специализированных программ обучения и специальных учебных планов, включая программы подготовки инструкторов и профессиональную сертификацию. Были признаны преимущества создания платформ для обмена информацией, включая передовую юридическую и административную практику, а также ценный вклад других соответствующих заинтересованных сторон в деятельность по наращиванию потенциала.

62. Государства пришли к выводу о том, что подведение итогов работы, проделанной государствами в связи с выводами и рекомендациями, содержащимися в

данном докладе, а также в связи с оценками и рекомендациями, которым государства-члены согласились следовать, приняв на основе консенсуса резолюцию 70/237, является ценным мероприятием для оценки прогресса и определения сфер, в которых требуется дальнейшее наращивание потенциала.

Рекомендации Рабочей группы открытого состава

63. Государствам следует руководствоваться принципами, изложенными в пункте 56, в своей связанной с ИКТ работе по наращиванию потенциала в сфере международной безопасности, а другим субъектам рекомендуется учитывать эти принципы в осуществляемой ими деятельности по наращиванию потенциала.

64. Государствам следует продолжать добровольно информировать Генерального секретаря о своих взглядах и оценках относительно достижений в области ИКТ в контексте международной безопасности и включать дополнительную информацию об извлеченном опыте и передовой практике в отношении программ и инициатив по наращиванию потенциала.

65. Государствам следует добровольно использовать модель «Обзор хода реализации на национальном уровне резолюции 70/237 Генеральной Ассамблеи Организации Объединенных Наций» (будет доступен в онлайн-режиме) для облегчения представления отчетности. Государства-члены, возможно, пожелают также добровольно использовать модель для структурирования информации в рамках своих вышеупомянутых документов, посредством которых они информируют Генерального секретаря о своих взглядах и оценках.

66. Государствам и другим субъектам, которые в состоянии предложить финансовую, ресурсную или техническую помощь в целях наращивания потенциала, следует делать это. Следует продолжать содействовать координации и обеспечению ресурсами усилий по наращиванию потенциала, в том числе с участием соответствующих организаций и Организации Объединенных Наций.

67. Государствам следует продолжать рассматривать вопрос о наращивании потенциала на многостороннем уровне, включая обмен мнениями, информацией и передовой практикой.

Регулярный институциональный диалог

68. РГОС, которая была создана во исполнение резолюции 73/27 Генеральной Ассамблеи, впервые позволила всем государствам провести под эгидой Организации Объединенных Наций специализированное обсуждение достижений в области ИКТ в контексте международной безопасности.

69. В дополнение к решению задачи добиться общего понимания между всеми государствами РГОС содействовала развитию дипломатических сетей и способствовала установлению доверительных отношений между участниками. Участие широкого круга неправительственных заинтересованных сторон продемонстрировало готовность более широкого сообщества субъектов использовать имеющуюся экспертную поддержку для оказания государствам помощи в решении стоящей перед ними задачи обеспечения открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Дискуссии, состоявшиеся в рамках РГОС, подтвердили важность регулярного и организованного обсуждения вопросов использования ИКТ под эгидой Организации Объединенных Наций.

70. Государства пришли к выводу о том, что регулярный диалог под эгидой Организации Объединенных Наций способствует достижению общих целей

укрепления международного мира, стабильности и предотвращения конфликтов в ИКТ-среде. Государства пришли также к выводу о том, что с учетом растущей зависимости от ИКТ и масштабов угроз, возникающих в результате их злонамеренного использования, существует срочная необходимость в дальнейшей работе по углублению общего понимания, укреплению доверия и активизации международного сотрудничества.

71. Поскольку государства несут главную ответственность за обеспечение национальной безопасности, общественного порядка и верховенства права, государства подтвердили важность регулярного межправительственного диалога и определения подходящих механизмов для взаимодействия с другими группами заинтересованных сторон в будущих процессах.

72. Рассмотрение в Организации Объединенных Наций вопроса о достижениях в сфере ИКТ и международной безопасности сосредоточено на аспектах их использования, которые связаны с международным миром, стабильностью и предотвращением конфликтов. Государства пришли к выводу о том, что планируемый в будущем регулярный институциональный диалог не должен дублировать существующие мандаты, усилия и мероприятия Организации Объединенных Наций, посвященные цифровым аспектам других вопросов[8]. Государства пришли к выводу о том, что установление более широкого обмена между этими форумами и процессами, инициированными Первым комитетом, могло бы способствовать повышению их взаимодополняемости и согласованности при одновременном соблюдении принципов экспертного характера или специализированного мандата каждого органа.

73. Государства пришли к выводу о том, что будущий диалог по вопросам международного сотрудничества в области ИКТ в контексте международной безопасности должен, в частности, способствовать повышению информированности, укреплению доверия и способствовать дальнейшему изучению и обсуждению тех областей, в отношении которых общее понимание еще не достигнуто. Государства признали пользу изучения механизмов, предназначенных для контроля за осуществлением согласованных норм и правил, а также для разработки дополнительных норм и правил.

74. Государства пришли к выводу о том, что любые будущие механизмы поддержания регулярного институционального диалога под эгидой Организации Объединенных Наций должны быть практико-ориентированным процессом с конкретными целями, который основан на достигнутых ранее результатах и носит инклюзивный, прозрачный, консенсусный и нацеленный на результаты характер.

Рекомендации Рабочей группы открытого состава

75. Государствам следует продолжать активно участвовать в регулярном институциональном диалоге под эгидой Организации Объединенных Наций.

76. Государствам следует обеспечить продолжение инклюзивного и прозрачного процесса переговоров по ИКТ в контексте международной безопасности

[8] См. справочный документ, подготовленный Председателем РГОС и озаглавленный “An Initial Overview of UN System Actors, Processes and Activities on ICT-related issues of Interest to the OEWG, By Theme”, декабрь 2019 года, URL: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-existing-un-bodies-processes-related-to-mandate.pdf.

под эгидой Организации Объединенных Наций, включая и признавая Рабочую группу открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, учрежденную в соответствии с резолюцией 75/240 Генеральной Ассамблеи.

77. Государствам следует принимать к сведению различные предложения по поощрению ответственного поведения государств в сфере ИКТ, которые, в частности, будут способствовать укреплению потенциала государств в выполнении обязательств по использованию ИКТ, в частности Программы действий. При рассмотрении таких предложений следует учитывать обеспокоенность и интересы всех государств путем обеспечения равноправного участия государств в деятельности Организации Объединенных Наций. В этой связи Программу действий следует доработать, в том числе в рамках процесса Рабочей группы открытого состава, учрежденной в соответствии с резолюцией 75/240 Генеральной Ассамблеи.

78. Государствам следует учитывать содержащиеся в настоящем докладе выводы и рекомендации во всех будущих процессах, связанных с регулярным институциональным диалогом под эгидой Организации Объединенных Наций.

79. Государствам, имеющим соответствующие возможности, следует рассмотреть вопрос о создании или поддержке спонсорских программ и других механизмов для обеспечения широкого участия в вышеупомянутых процессах в рамках Организации Объединенных Наций.

C. Заключительные положения

80. Государства последовательно и активно участвовали в РГОС на протяжении всего процесса, что позволило провести крайне плодотворный обмен мнениями. Отчасти ценность такого обмена заключается в том, что были высказаны различные точки зрения, новые идеи и важные предложения, включая возможность принятия дополнительных юридически обязательных обязательств, хотя и не все государства поддержали их. Различные точки зрения представлены в прилагаемом резюме Председателя по итогам дискуссий и обсуждения конкретных предложений по формулировкам в рамках пункта повестки дня «Правила, нормы и принципы». Эти точки зрения следует дополнительно изучить в рамках будущих процессов под эгидой Организации Объединенных Наций, в том числе в Рабочей группе открытого состава, созданной в соответствии с резолюцией 75/240 Генеральной Ассамблеи.

Приложение II*

Резюме Председателя

A. Контекст

1. РГОС предоставила всем государствам историческую возможность на равных основаниях принять участие в проводимом под эгидой Организации Объединенных Наций целенаправленном и непрерывном обсуждении вопросов, связанных с ИКТ в контексте международной безопасности. Проведение всеохватных и прозрачных обсуждений в рамках Рабочей группы открытого состава не только позволило достичь согласия по многим вопросам, отраженным в ее докладе, но и стало ценной мерой укрепления международного мира и безопасности благодаря повышению доверия и углублению взаимопонимания между государствами, а также помогло создать глобальную дипломатическую сеть национальных экспертов. Активное и широкое участие всех делегаций продемонстрировало решимость государств продолжать совместную работу по этому вопросу, имеющему основополагающее значение для всех.

2. Отличительным признаком всех заседаний РГОС стал интерактивный обмен мнениями по вопросам существа с участием государств, а также гражданского общества, частного сектора, научных кругов и технического сообщества. Решимость, которую государства и другие заинтересованные стороны продемонстрировали на всем протяжении работы РГОС, и готовность работать даже в условиях перевода некоторых заседаний Группы в виртуальный формат являются бесспорным доказательством все более универсальной значимости рассматриваемых ею тем, а также растущего признания насущной необходимости коллективно противодействовать угрозам международной безопасности, которые возникают вследствие злонамеренного использования ИКТ.

3. В настоящем резюме, ответственность за опубликование которого несет Председатель, представлено его понимание основных вопросов, которые обсуждались на заседаниях Рабочей группы открытого состава. В нем может быть представлена не вся информация об участии в работе всех делегаций, и его не следует рассматривать как документ с изложением консенсусной точки зрения государств по каким-либо конкретным вопросам, которые в нем затрагиваются. Полная подборка заявлений и предложений государств, которые были представлены для распространения, размещена на веб-сайте https://www.un.org/disarmament/open-ended-working-group.

B. Обзор хода обсуждений

4. Процесс РГОС предоставила всем государствам возможность высказать свою точку зрения, обеспокоенность или пожелания в демократичном, прозрачном и инклюзивном ключе. Хотя РГОС стремилась определить сферы близости позиций и консенсуса, обсуждения в ней также свидетельствуют о разнообразии высказанных государствами-членами мнений, идей и предложений и могут послужить полезной основой для будущей работы, направленной на дальнейшее углубление общего понимания по вопросам использования ИКТ государствами в контексте международной безопасности.

* Публикуется без официального редактирования.

5. В ходе обсуждений в РГОС государства подчеркивали взаимосвязанный и взаимоусиливающий характер всех элементов ее мандата. Так, международное право регулирует действия государств и их отношения, а добровольные, не имеющие обязательной силы нормы содержат дополнительные указания в отношении того, что представляет собой ответственное поведение государства. Оба этих элемента отражают ожидания в отношении поведения государств в связи с использованием ИКТ в контексте международной безопасности. Тем самым они также способствуют укреплению доверия за счет повышения прозрачности и развития сотрудничества между государствами и уменьшению риска возникновения конфликтов. В свою очередь укрепление потенциала позволяет всем государствам содействовать укреплению стабильности и безопасности во всем мире. В совокупности эти элементы составляют глобальные рамки для принятия совместных мер по устранению существующих и потенциальных угроз в области ИКТ. Регулярный институциональный диалог даст возможность продолжить развитие и практическое использование этой основы за счет углубления общего понимания, обмена извлеченными уроками и передовой практикой в области осуществления, укрепления доверия между государствами и укрепления потенциала всех государств.

Существующие и потенциальные угрозы

6. В ходе обсуждений в РГОС государства затронули широкий круг существующих и потенциальных угроз, что наглядно показало, что государства могут поразному воспринимать угрозы, исходящие из ИКТ-среды. Инклюзивный формат работы РГОС предоставил государствам возможность глубже понять, как действия и поведение в ИКТ-среде воспринимается другими, а также ознакомиться с мнениями других о том, что они считают наиболее значительными угрозами и рисками.

7. Некоторые государства выразили озабоченность по поводу разработки или использования ИКТ в целях, несовместимых с целями поддержания международного мира и безопасности. Некоторые из них были озабочены тем, что особенности ИКТ-среды могут способствовать не столько урегулированию споров мирными средствами, сколько принятию односторонних мер. Некоторые государства отметили свою озабоченность по поводу развития потенциала ИКТ в военных и других подобных целях, что может подорвать международный мир и безопасность. Другие государства отметили, что угроза заключается в использовании государствами такого потенциала вопреки их обязательствам по международному праву. Была также выражена озабоченность по поводу накопления факторов уязвимости и отсутствия прозрачности и четко определенных процедур для раскрытия информации о них, использования вредоносных скрытых функций, целостности глобальных цепочек поставок в области ИКТ и обеспечения безопасности данных. Некоторые государства выразили обеспокоенность по поводу того, что ИКТ могут использоваться для вмешательства в их внутренние дела, в том числе посредством информационных операций и кампаний по распространению дезинформации. В качестве конкретной проблемы было названо стремление к повышению уровня автоматизации и автономии операций в сфере ИКТ, а также принятие мер, которые могут привести к ограничению или нарушению связи, непреднамеренной эскалации или негативным последствиям для третьих сторон. В качестве отдельной проблемы некоторые государства также отметили отсутствие ясности в отношении обязанностей частного сектора.

8. Государства особо отметили, что меры, направленные на поощрение ответственного поведения государств, должны оставаться нейтральными с технической точки зрения, подчеркнув при этом, что проблемой являются не сами технологии, а их ненадлежащее использование. Государства признали, что даже с учетом того, что технический прогресс и новые прикладные программы могут открывать возможности для развития, они могут также способствовать расширению сферы нападений, усиливать уязвимость ИКТ-среды или использоваться для осуществления новых видов злонамеренной деятельности. В этой связи отмечались конкретные направления развития техники и технические достижения, в том числе прогресс в области машинного обучения и квантовых вычислений, повсеместное использование подключенных устройств («Интернет вещей»), новые способы хранения и получения данных с использованием технологий распределенного реестра и облачных вычислений, и бурный рост объема больших данных и оцифрованных личных данных.

Международное право

9. Действуя в рамках мандата Группы и преследуя цель поддержания мира и стабильности и содействия созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды и поощрения общего понимания, государства провели обмен мнениями о том, как международное право применяется к вопросам, касающимся ИКТ в контексте международной безопасности.

10. В ходе обсуждений в РГОС государства напомнили, что международное право, и в частности Устав Организации Объединенных Наций во всей своей полноте, применимо и имеет ключевое значение для поддержания мира и стабильности и содействия обеспечению открытой, безопасной, стабильной, мирной и доступной ИКТ-среды. В этой связи государства особо отметили, что необходимо предпринимать шаги к тому, чтобы не допускать и воздерживаться от введения любых мер, не соответствующих Уставу Организации Объединенных Наций и международному праву и препятствующих всестороннему обеспечению экономического и социального развития населения затрагиваемых стран и подрывающих их благосостояние. В то же время государства подчеркнули также, что вопрос о том, как международное право применяется к использованию ИКТ государствами, требует дальнейшей проработки.

11. В ходе обсуждений были подтверждены конкретные принципы международного права, включая, среди прочего, государственный суверенитет, суверенное равенство, разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость, отказ в международных отношениях от применения силы или угрозы силой как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями Организации Объединенных Наций, уважение прав человека и основных свобод и невмешательство во внутренние дела других государств.

12. Было вновь отмечено, что международное право является основой стабильности и предсказуемости в отношениях между государствами. В частности, снижению рисков и уменьшению потенциального ущерба для гражданских лиц и гражданских объектов, а также комбатантов в контексте вооруженного конфликта способствует международное гуманитарное право. В то же время государства подчеркнули, что международное гуманитарное право не поощряет

милитаризацию и не легитимизирует применение силы в какой бы то ни было области.

13. Было также отмечено, что в соответствии с обычным международным правом ответственность государств за международно-противоправные деяния распространяется на использование ИКТ.

14. Было вновь отмечено, что государства не должны использовать посредников для совершения международно-противоправных деяний с применением ИКТ и должны стремиться обеспечить, чтобы их территория не использовалась для совершения таких деяний негосударственными субъектами, действующими по указанию государства или под его контролем. Была также отмечена ответственность государств в отношении субъектов, принадлежащих государству или находящихся под его контролем.

15. Государства вновь отметили, что указания на то, что та или иная деятельность в сфере ИКТ была начата или иным образом осуществляется с территории или объектов ИКТ-инфраструктуры государства, может быть недостаточно для присвоения этой деятельности указанному государству и что обвинения в организации и совершении противоправных деяний, выдвигаемые против государств, должны быть обоснованными. Некоторые государства подчеркнули важность подлинных, надежных и достаточных доказательств в этом контексте.

16. По мнению некоторых государств, существующих норм международного права, дополняемых добровольными, не имеющими обязательной силы нормами, которые отражают консенсус между государствами, в настоящее время достаточно для решения вопросов, связанных с использованием ИКТ государствами. Было также предложено сосредоточить усилия на достижении общего понимания в отношении того, каким образом уже согласованные нормативные рамки применяются путем развития дополнительных руководящих принципов и могут быть операционализированы посредством поощрения их соблюдения всеми государствами. В то же время другие государства высказали мнение о том, что ввиду быстро меняющегося характера угроз и серьезности риска необходимы согласованные на международном уровне и имеющие обязательную юридическую силу нормативные рамки использования ИКТ. Была также высказана мысль о том, что такие имеющие обязательную силу нормативные рамки могут способствовать более эффективному выполнению обязательств на глобальном уровне и могут стать более надежной основой для привлечения субъектов к ответственности за совершенные действия. Государства подчеркнули, что при разработке любых международно-правовых рамок для решения проблем, вызванных таким использованием ИКТ, которое может иметь последствия для международного мира и безопасности, следует учитывать озабоченность и интересы всех государств, руководствоваться правилом консенсуса, и что этим следует заниматься в рамках Организации Объединенных Наций при активном и равноправном участии в нем всех государств.

17. Было подчеркнуто, что, хотя существующие инструменты международного права не содержат конкретных ссылок на использование ИКТ в контексте международной безопасности, международное право может прогрессивно развиваться, в том числе на основе принципа opinion juris и практики государств. Был поднят вопрос о возможности постепенной разработки одновременно с применением норм дополнительных обязательных мер. Кроме того, было высказано предложение о том, что одним из возможных направлений могло бы стать принятие политического обязательства.

18. Напомнив о том, что международное право, и в частности Устав Организации Объединенных Наций, применимы к использованию ИКТ, было подчеркнуто, что некоторые вопросы, касающиеся применимости международного права к использованию ИКТ, еще предстоит прояснить в полной мере. Некоторые государства предложили отнести к таким вопросам, среди прочего, такие виды связанной с ИКТ деятельности, которые могут быть истолкованы другими государствами как угроза силой или ее применение (статья 2 (4) Устава) или могут дать государству основание воспользоваться своим неотъемлемым правом на самооборону (статья 51 Устава). Кроме того, речь идет о вопросах, связанных с тем, как принципы международного гуманитарного права, такие как гуманность, необходимость, соразмерность, различие и предосторожность, применяются к операциям с использованием ИКТ. В связи с этим некоторые государства отметили необходимость осмотрительного подхода к обсуждению вопроса о применимости международного гуманитарного права к использованию ИКТ государствами. Государства отметили необходимость дальнейшего изучения этих важных тем в ходе будущих обсуждений.

19. Кроме того, в перспективе, по предложению государств, одним из важнейших первых шагов по уточнению и дальнейшему углублению общего понимания могло бы стать расширение обмена мнениями и углубленное обсуждение государствами вопроса о том, как международное право применяется к использованию ИКТ государствами. Было отмечено, что такой обмен мнениями сам по себе может служить важной мерой укрепления доверия. Кроме того, некоторые государства предложили несколько способов добровольного обмена национальными мнениями о том, как применяется международное право, включая использование ежегодного доклада Генерального секретаря о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности[9], портала по вопросам киберполитики Института Организации Объединенных Наций по исследованию проблем разоружения или использование обзора национальной практики применения международного права. Были также отмечены позитивные результаты, достигнутые в реализации региональных и других договоренностей об обмене мнениями и выработке общего понимания в отношении того, как применяется международное право.

20. Что касается вопроса о поддержании мира и предотвращении конфликтов, то государства подтвердили необходимость урегулировать споры мирными средствами и воздерживаться от угрозы силой или ее применения. В этой связи государства напомнили о существующих органах, механизмах и средствах предупреждения и мирного урегулирования споров. Некоторые государства высказали мысль о том, что разработка под эгидой Организации Объединенных Наций пользующегося универсальным признанием общего подхода и понимания источника инцидентов в сфере ИКТ на техническом уровне на основе обмена передовым опытом с учетом уважения принципа государственного суверенитета могла бы привести к повышению подотчетности и прозрачности и могла бы способствовать применению средств правовой защиты теми, кому в результате злонамеренных действий был причинен ущерб.

Правила, нормы и принципы ответственного поведения государств

21. В ходе обсуждений в рамках РГОС государства напомнили о том, что добровольные, не имеющие обязательной силы нормы ответственного поведения

[9] Резолюция 75/32 Генеральной Ассамблеи.

государств не изменяют и не подменяют собой международное право и цели и принципы Организации Объединенных Наций, включая поддержание международного мира и безопасности и поощрение прав человека, а должны рассматриваться как соответствующие международному праву и целям и принципам Организации Объединенных Наций. Государства также отметили резолюцию 2131 (XX) Генеральной Ассамблеи 1965 года, озаглавленную «Декларация о недопустимости вмешательства во внутренние дела государств, об ограждении их независимости и суверенитета».

22. Государства сослались на резолюцию 73/27 Генеральной Ассамблеи, которая содержит перечень из 13 правил, норм и принципов ответственного поведения государств и, помимо прочего, подтверждает 11 добровольных, не имеющих обязательной силы норм, «закрепленных в докладах групп правительственных экспертов Организации Объединенных Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2013 и 2015 годов, принятых консенсусом и рекомендованных резолюцией 71/28»[10].

23. Государства подчеркнули необходимость повышения осведомленности о существующих нормах и поддержки их операционализации одновременно с разработкой новых норм. Государства подчеркнули необходимость выработки указаний в отношении того, как эти нормы должны операционализироваться. В этой связи государства призвали обмениваться передовым опытом и извлеченными уроками в отношении имплементации норм и распространять такой опыт и уроки. Для содействия усилиям государств по имплементации были предложены различные подходы, основанные на сотрудничестве, такие как разработка государствами дорожной карты и добровольное анкетирование в целях обмена опытом и передовой практикой.

24. Государства отметили, что нормы могут способствовать предотвращению конфликтов в ИКТ-среде и способствовать использованию ИКТ в мирных целях и полной реализации выгод от их использования в целях ускорения социального и экономического развития во всем мире. Государства подчеркнули, что применение норм не должно приводить к неоправданным ограничениям для международного сотрудничества и передачи технологий, а также не должно препятствовать инновациям в мирных целях и экономическому развитию государств в условиях справедливости и недискриминации. Государства также подчеркнули, что между нормами, укреплением доверия и наращиванием потенциала существует взаимосвязь, и указали на необходимость уделять значительное внимание гендерным факторам при применении норм.

25. В ходе обсуждений высказывались предложения в отношении дальнейшей разработки существующих норм. Государства вновь заявили также о важности защиты всех объектов критически важной инфраструктуры, которые обеспечивают оказание основных услуг населению и к которым следует относить медицинские и здравоохранительные учреждения. С учетом потенциальных последствий причинения любого ущерба объектам критически важной инфраструктуры, которые используются для предоставления трансграничных или международных услуг, государства обратили также внимание на важность сотрудничества в защите таких объектов, а также на важность обеспечения общедоступности и целостности Интернета. Государства сослались на резолюцию 64/211 Генеральной Ассамблеи «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных

[10] Резолюция 73/27 Генеральной Ассамблеи, пункт 1 постановляющей части.

инфраструктур»[11]. Кроме того, государства, выразив обеспокоенность по поводу включения в ИКТ-продукты вредоносных скрытых функций, также предложили дополнительно обеспечить надежность цепочки поставок ИКТ и ответственность за уведомление пользователей при выявлении серьезных факторов уязвимости. Более того, государства выразили озабоченность по поводу накопления факторов уязвимости. Некоторые государства предложили сформулировать объективные международные правила и стандарты безопасности цепочек поставок.

26. В дополнение к сказанному в приложении к настоящему резюме представлены письменные предложения государств по доработке существующих норм, разработке указаний по их применению и выработке новых норм.

27. Некоторые государства также отметили представленное в 2015 году предложение о разработке международного кодекса поведения в области информационной безопасности[12].

28. Некоторые государства признали необходимость поощрять и поддерживать дополнительные усилия на региональном уровне, а также налаживать партнерские отношения с другими заинтересованными сторонами, например с частным сектором и техническим сообществом, по вопросам применения норм. Такие партнерские отношения можно было бы выстраивать, например, для обеспечения того, чтобы усилия по наращиванию потенциала для устранения различий в возможностях в плане имплементации норм носили устойчивый характер. В этой связи государства сослались на пункт 1.13 постановляющей части резолюции 73/27 Генеральной Ассамблеи, в котором, в частности, подчеркивается, что «государства должны содействовать тому, чтобы частный сектор и гражданское общество играли надлежащую роль в укреплении безопасности при использовании ИКТ и самих ИКТ, включая безопасность всей системы производства и сбыта информационных товаров и информационно-технических услуг». Государства отметили важное значение информационно-разъяснительной работы и принятия совместных мер для обеспечения того, чтобы различные заинтересованные стороны, включая государственный и частный сектор и гражданское общество, выполняли свои обязанности в связи с использованием ИКТ.

Меры укрепления доверия

29. В ходе обсуждений в рамках РГОС государства отметили сохраняющуюся актуальность мер укрепления доверия, рекомендованных в консенсусных докладах группы правительственных экспертов. Был отмечен ряд мер, требующих первоочередного внимания, таких как регулярный диалог и добровольный обмен информацией о существующих и потенциальных угрозах, национальной политике, законодательной базе или доктринах, национальных взглядах на то, как международное право применяется к использованию ИКТ государствами, а также о национальных подходах к определению критически важной инфраструктуры и классификации происшествий, связанных с ИКТ. Было высказано мнение о том, что обмен передовым опытом в области цифровой криминалистики и расследования инцидентов, связанных со злонамеренными действиями в киберпространстве, мог бы способствовать как укреплению сотрудничества, так и наращиванию потенциала. Была также подчеркнута важность выработки

[11] В приложении к этой резолюции содержится инструмент добровольной самооценки национальных усилий по защите объектов критически важной информационной инфраструктуры.

[12] Документ A/69/723, упоминаемый в п. 12 документа A/70/174.

общего понимания концепций и терминологии в качестве одной из практических мер, направленных на развитие международного сотрудничества и укрепление доверия. К числу других таких мер относятся разработка руководства по имплементации мер укрепления доверия, подготовка дипломатов, обмен опытом создания и использования защищенных каналов связи в кризисных ситуациях, обмен персоналом, проведение учений на основе сценариев на директивном уровне, а также оперативные учения на техническом уровне по линии групп реагирования на компьютерные инциденты (CERTs) и групп реагирования на инциденты в сфере компьютерной безопасности (CSIRTs). Было высказано предложение о том, что еще одним направлением деятельности по укреплению доверия и повышению уверенности в отношении намерений и обязательств государств могут быть национальные меры обеспечения прозрачности, такие как участие в добровольном анкетировании о ходе имплементации или публикация национальных заявлений о соблюдении рамок ответственного поведения государств.

30. Была рассмотрена возможность создания централизованного глобального реестра контактных пунктов с учетом накопленного региональными органами опыта создания и поддержания функционирования сетей контактных пунктов и на основе существующих сетей. В то же время было отмечено, что решающее значение для эффективности такого реестра будут иметь не только его безопасность и порядок его функционирования, но и то, насколько удастся избежать дублирующих или чрезмерно детализованных процедур. Была также подчеркнута значимость регулярного проведения учений в рамках сети контактных центров, поскольку это может способствовать поддержанию готовности и повышению оперативности, а также обеспечению постоянного обновления реестров контактных пунктов.

31. Поскольку меры укрепления доверия могут разрабатываться на двустороннем, региональном или многостороннем уровнях, государства также обсудили желательность и целесообразность создания глобальной базы данных о мерах укрепления доверия под эгидой Организации Объединенных Наций, с тем чтобы обеспечить обмен информацией о политике, передовой практике, опыте и анализе осуществления мер укрепления доверия и содействовать взаимному обучению и направлению средств на наращивание потенциала. Такая база могла бы также помочь государствам в определении дополнительных мер укрепления доверия, которые бы отвечали их национальным и региональным условиям, и быть адаптирована для использования в других областях. Было отмечено, что любая создаваемая глобальная база данных не должна дублировать существующие механизмы и что условия функционирования такой базы требуют дальнейшего обсуждения.

32. Государства также обратили внимание на функции и обязанности других субъектов, включая гражданское общество, частный сектор, научные круги и техническое сообщество, в деле содействия укреплению доверия и повышения уверенности в связи с использованием ИКТ на национальном, региональном и глобальном уровнях. Государства отметили разнообразие инициатив с участием многих заинтересованных сторон, благодаря которым на основе разработки принципов и обязательств были созданы новые сети для обмена информацией, взаимодействия и сотрудничества. Точно так же инициативы в конкретных секторах или областях демонстрируют растущее понимание функций и обязанностей других участников и тот уникальный вклад, который они могут внести в

обеспечение безопасности ИКТ благодаря добровольным обязательствам, кодексам профессионального поведения и стандартам.

Наращивание потенциала

33. В ходе обсуждений в рамках РГОС государства отметили, что наращивание потенциала может играть важную роль в предоставлении всем государствам возможности в полной мере участвовать в обсуждении на международном уровне рамок ответственного поведения государств, способствуя при этом выполнению таких совместных обязательств, как Повестка дня в области устойчивого развития на период до 2030 года[13]. В этой связи государства подчеркнули необходимость обеспечения программ по наращиванию потенциала достаточными финансовыми и кадровыми ресурсами.

34. Государства отметили важную работу, проводимую в области наращивания потенциала, связанного с ИКТ, другими субъектами, включая международные организации, региональные и субрегиональные органы, гражданское общество, частный сектор, научные круги и специализированные технические органы, и призвали подумать над тем, как содействовать координации, поступательному характеру, эффективности и сокращению дублирования всех этих усилий.

35. Организация Объединенных Наций призвана сыграть важную роль в оказании государствам поддержки в повышении значимости деятельности по наращиванию потенциала и в поддержке более тесной координации деятельности различных субъектов, занимающихся вопросами наращивания потенциала, на основе использования ее организаторских возможностей. Государства предложили использовать существующие платформы в рамках Организации Объединенных Наций, ее специализированных учреждений и международного сообщества в целом для укрепления уже налаженной координации. Эти платформы можно было бы использовать для обмена национальными мнениями о потребностях в наращивании потенциала, содействия распространению выводов и опыта как получателями, так и поставщиками помощи и облегчения доступа к информации о программах наращивания потенциала и оказания технической помощи. Эти платформы могли бы также способствовать мобилизации ресурсов или содействовать направлению имеющихся ресурсов для удовлетворения просьб об оказании поддержки в создании потенциала и технической помощи. Была высказана мысль о том, что разработка под эгидой Организации Объединенных Наций глобальной программы наращивания потенциала в области ИКТ могла бы способствовать повышению слаженности усилий по наращиванию потенциала и что добровольное анкетирование для оценки своей деятельности может помочь государствам в выявлении и определении важности потребностей в области наращивания потенциала или возможностей в области оказания поддержки.

36. Одновременно с главной ответственностью государств за поддержание безопасной, надежной и пользующейся доверием ИКТ-среды была также подчеркнута важность основанного на участии множества заинтересованных

[13] К соответствующим целям и задачам в области устойчивого развития относятся, в частности, существенное расширение доступа к информационно-коммуникационным технологиям (9.C), расширение сотрудничества по линии Север — Юг и Юг — Юг, а также трехстороннего регионального и международного сотрудничества в областях науки, техники и новаторства и доступа к соответствующим достижениям (17.6) и усиление международной поддержки эффективного и целенаправленного наращивания потенциала (17.9).

сторон подхода к наращиванию потенциала, позволяющего устранять технические и нормативные недостатки во всех соответствующих секторах общества. Государства отметили, в частности, что поступательный характер деятельности по наращиванию потенциала может быть обеспечен с помощью подхода, предполагающего взаимодействие и партнерство с местным гражданским обществом, техническим сообществом, научно-образовательными учреждениями и субъектами частного сектора, а также за счет создания реестров экспертов и специализированных узловых центров. В этой связи было также подчеркнуто, что благоприятное воздействие на национальные подходы к безопасности ИКТ могло бы оказать принятие межсекторального, целостного и междисциплинарного подхода к наращиванию потенциала, в том числе путем укрепления национальных координационных органов с участием соответствующих заинтересованных сторон для оценки эффективности программ. Такой подход может также способствовать решению проблем, возникающих в связи с появлением новых технологий.

37. Государства обратили внимание на гендерный цифровой разрыв и настоятельно призвали принять конкретные меры на национальном и международном уровнях для решения проблемы гендерного неравенства и обеспечения конструктивного участия женщин в международных дискуссиях и программах по наращиванию потенциала в области ИКТ и международной безопасности, в том числе путем сбора данных, дезагрегированных по гендерному признаку. Государства дали высокую оценку программам, которые способствуют участию женщин в многосторонних обсуждениях по вопросам безопасности ИКТ. Была также подчеркнута необходимость укрепления связи этой темы с повесткой дня Организации Объединенных Наций по вопросам женщин, мира и безопасности.

38. Государства отметили, что существуют многочисленные факторы, которые препятствуют повышению эффективности деятельности по наращиванию потенциала или снижают ее эффективность. В качестве серьезных проблем были отмечены недостаточная координация и взаимодополняемость при выборе направлений и осуществлении деятельности по наращиванию потенциала. Государства также подняли вопросы практического характера, касающиеся определения потребностей в наращивании потенциала, оперативного реагирования на просьбы об оказании помощи в наращивании потенциала, а также разработки, осуществления, устойчивости и доступности мероприятий по наращиванию потенциала и отсутствия конкретных показателей для измерения их воздействия. Во многих случаях деятельность по наращиванию потенциала и прогресс в деле сокращения цифрового разрыва затрудняются отсутствием достаточных кадровых, финансовых и технических ресурсов. После того как задача наращивания потенциала уже решена, некоторые страны сталкиваются с проблемой удержания квалифицированных кадров в условиях повышенного спроса на ИКТ-специалистов. Государства отметили, что еще одной проблемой является отсутствие доступа к технологиям, связанным с обеспечением безопасности ИКТ.

Регулярный институциональный диалог

39. В ходе состоявшихся в Рабочей группе открытого состава обсуждений государства напомнили о содержащемся в резолюции 73/27 Генеральной Ассамблеи мандате Рабочей группы изучить возможность организации регулярного институционального диалога и подтвердили, что одним из ключевых результатов работы Группы станут подготовленные ею оценки и рекомендации.

40. Государства высказали ряд мнений относительно целей, которые должны стать приоритетными для будущего регулярного институционального диалога, и относительно того, какой формат регулярного диалога мог бы наилучшим образом способствовать достижению этих целей. Некоторые государства выразили желание, чтобы в рамках регулярного диалога приоритетное внимание уделялось выполнению существующих обязательств и рекомендаций, включая разработку руководящих указаний по поддержке и проверке их выполнения, координации и повышению эффективности деятельности по наращиванию потенциала и определению передового опыта и обмену им. Другие государства выразили пожелание, чтобы в рамках регулярного диалога приоритетное внимание уделялось дальнейшей проработке существующих обязательств и выработке дополнительных обязательств, включая согласование юридически обязывающего инструмента и институциональных структур в поддержку его применения.

41. Некоторые государства внесли конкретное предложение о разработке Программы действий по поощрению ответственного поведения государств в киберпространстве с целью создания постоянного форума Организации Объединенных Наций для рассмотрения вопросов использования ИКТ государствами в контексте международной безопасности. Было предложено отразить в Программе действий политическое обязательство государств следовать согласованным рекомендациям, нормам и принципам, проводить регулярные встречи по вопросам имплементации, укреплять сотрудничество между государствами и активизировать их деятельность по наращиванию потенциала и проводить регулярные обзорные конференции. В рамках Программы действий было также предложено обеспечить участие широкого круга сторон и проведение консультаций.

42. Государства отметили учреждение в соответствии с резолюцией 75/240 от 31 декабря 2020 года новой Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, которая начнет функционировать по завершении деятельности Рабочей группы открытого состава, учрежденной во исполнение резолюции 73/27, и рассмотрит результаты ее работы.

43. Государства также выразили пожелание, чтобы международное сообщество в конечном счете вернулось к единому основанному на консенсусе процессу под эгидой Организации Объединенных Наций. В этой связи государства отметили, что различные предлагаемые форматы диалога не обязательно являются взаимоисключающими. Была высказана мысль о том, что различные форматы могут дополнять друг друга или могут быть объединены, с тем чтобы использовать уникальные особенности каждого из них и сократить дублирование усилий.

44. Кроме того, была отмечена необходимость продолжить рассмотрение вопроса о сроках и устойчивости будущего диалога, а также были подняты вопросы, касавшиеся выбора между консультативным и ориентированным на практические действия характером диалога, сроков и возможных мест его проведения и бюджетных соображений.

45. Признав уникальную роль и ответственность государств в обеспечении национальной и международной безопасности, государства подчеркнули, что ответственное поведение других субъектов в немалой степени способствует созданию открытой, безопасной, доступной и мирной ИКТ-среды. В этой связи было отмечено, что формированию более устойчивой и безопасной ИКТ-среды может способствовать расширение сотрудничества и партнерских связей с участием многих заинтересованных сторон.

Приложение к резюме Председателя

Конкретные предложения относительно формулировок по пункту повестки дня «Правила, нормы и принципы» из материалов, представленных делегациями в письменном виде

С учетом того, что в своих письменных материалах многие делегации ссылались на существующие нормы, ниже приводятся лишь дополнительные предложения относительно формулировок.

Армения

- Государства будут воздерживаться от любых действий, которые могут привести к попыткам нарушения целостности критической инфраструктуры и деятельности правительства, а также направлять по защищенным каналам своевременные разъяснения для предотвращения дальнейшей возможной эскалации.

Австралия, Казахстан, Соединенные Штаты Америки, Чешская Республика, Эстония и Япония

Текст с указаниями по имплементации норм в пунктах 13 f) и g) доклада 2015 года

- При подготовке указаний относительно имплементации этих норм государства должны учитывать, что выделение определенных секторов в качестве критической инфраструктуры не предполагает составления исчерпывающего перечня и не влияет на определение государством какого-либо другого сектора в качестве критически важного, а также не означает косвенного попустительства в отношении злонамеренных действий против какой-либо категории, не включенной в такой перечень.
- РГОС готовила свой доклад в условиях пандемии COVID-19. В этих обстоятельствах РГОС подчеркнула, что все государства рассматривают медицинские службы и медицинские учреждения в качестве критической инфраструктуры для целей норм f) и g).

Беларусь

- Государства должны вновь подтвердить свою приверженность принципу отказа от милитаризации существующих ИКТ и от создания новых ИКТ, специально предназначенных для нанесения ущерба информационным ресурсам, инфраструктуре и критически важным объектам других стран.

Канада

Предлагаемый текст указания по имплементации норм для включения в пункт 41

Хотя в нормах, подготовленных ГПЭ в 2015 году, определены меры, которые государства должны и не должны принимать, государства подчеркнули необходимость в указаниях по их операционализации и предложили следующие указания в отношении этих норм. В понимании РГОС эти нормы и указания никак не

ущемляют существующие права и обязательства государств по международному праву и никоим образом не изменяют и не умаляют их.

a. 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, признаваемых вредоносными или способных создать угрозу международному миру и безопасности (2015 ¶13 a)).

i. Настоящая норма носит общий характер. Имплементация всего комплекса норм, а также изложенных ниже конкретных указаний будет способствовать дальнейшей операционализации этой нормы. Государства придерживаться подхода, основанного на сотрудничестве, в работе друг с другом и с негосударственными заинтересованными сторонами, включая представителей промышленности, научного сообщества и гражданского общества.

ii. Для этого государства должны по мере необходимости и по возможности делать следующее:

– принимать и реализовывать всеобъемлющие национальные стратегии в области кибербезопасности. Это должно по возможности способствовать международному сотрудничеству в сфере кибербезопасности;

– создавать и поддерживать механизмы реагирования на инциденты, например группы реагирования на компьютерные инциденты (CERTs), которые способны координировать свои действия, обмениваться передовым опытом и сотрудничать в реагировании на инциденты в сфере использования ИКТ;

– публиковать заявления о том, что они будут действовать в рамках норм ответственного поведения государств в киберпространстве, сформулированных в докладе, подготовленном в 2015 году ГПЭ;

– принимать участие в региональных и двусторонних инициативах, направленных на разработку и имплементацию мер укрепления доверия.

iii. Следует рекомендовать государствам-членам собирать и систематизировать информацию об имплементации ими принятых норм, которую они должны представлять.

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 (2015 ¶13 b)).

i. Государства могли бы учредить национальные структуры, разработать директивные документы и процессы и создать координационные механизмы, необходимые для содействия тщательному рассмотрению серьезных инцидентов в сфере использования ИКТ и определения надлежащих мер реагирования.

ii. После создания этих структур и разработки соответствующих процессов государства могли бы разработать шаблоны для описания инцидентов в сфере ИКТ и степени их значимости, с тем чтобы оценивать и анализировать инциденты в сфере использования ИКТ.

iii. Обеспечение прозрачности и унификации таких шаблонов региональными организациями могло бы гарантировать общность подходов государств к рассмотрению инцидентов в сфере использования ИКТ и улучшить коммуникацию между государствами. Такие шаблоны должны по возможности соответствовать сложившейся практике и не дублировать уже существующие формы.

iv. При рассмотрении всей значимой информации, касающейся того или иного инцидента в сфере использования ИКТ, государствам следует изучать возможные гендерно дифференцированные последствия и взаимодействовать со всеми заинтересованными сторонами, с тем чтобы понять более широкий контекст инцидента в сфере использования ИКТ, включая его воздействие на реализацию прав женщин и ЛГБТ-сообщества.

v. Государствам следует рассматривать воздействие инцидентов в сфере использования ИКТ на права человека, включая права на свободное выражение мнений и свободу ассоциаций и мирных собраний, право на свободу от произвольного или незаконного вмешательства в частную жизнь, а также права людей с ограниченными возможностями.

vi. Государствам следует признать, что реагирование на инциденты в сфере безопасности зачастую требует участия различных заинтересованных сторон, а не только национальных CERTs/CSIRTs, и развивать взаимодействие со всеми группами заинтересованных сторон посредством подготовки кадров и наращивания потенциала. Государствам следует поощрять участие заинтересованных кругов, включая гражданское общество, в подготовке специалистов по вопросам цифровой безопасности и другой деятельности по наращиванию потенциала и оказанию содействия в целях предотвращения инцидентов в сфере безопасности, особенно затрагивающих уязвимые группы населения и других пользователей в зоне риска.

c. Государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ (2015 ¶13 c)).

i. Замечания относительно имплементации данной нормы:

– Если государство выявляет злонамеренную активность с использованием киберсредств, исходящую с территории или с использованием киберинфраструктуры другого государства, то первым шагом может стать направление этому государству соответствующего уведомления. Ключевую роль в выявлении такой активности играют группы реагирования на компьютерные инциденты (CERTs).

– С учетом того, что инциденты в сфере ИКТ могут совершаться с территории третьих государств или при их участии, следует понимать, что направление уведомления тому или иному государства не означает возложения на это государство ответственности за инцидент.

– Получившее уведомление государство должно подтвердить получение запроса через соответствующий национальный контактный пункт.

– Когда государству известно, что его территория или киберинфраструктура используется для осуществления противоправных действий международного характера с использованием ИКТ, которые могут привести к серьезным неблагоприятным последствиям в другом государстве, первому государству следует попытаться принять разумные, доступные и практически осуществимые меры в пределах своей территории и возможностей в соответствии со своими обязательствами согласно внутреннему и международному праву, с тем чтобы пресечь такие противоправные действия международного характера или смягчить их последствия.

– Государство может узнать о таких действиях после получения уведомления от затронутого государства. Такое уведомление должно быть сделано добросовестно и содержать подтверждающую информацию. Подтверждающая информация может включать индикаторы компрометации, такие как IP-адрес и данные компьютера, использованного для совершения злонамеренных действий с использованием ИКТ, и сведения о вредоносных программах.

– Следует поощрять государства к обеспечению того, чтобы негосударственные субъекты, включая частный сектор, не могли осуществлять злонамеренную деятельность с использованием ИКТ в своих собственных целях или в целях государственных или других негосударственных субъектов в ущерб третьим сторонам, в том числе находящимся на территории другого государства. Эта цель может быть достигнута посредством определения в сотрудничестве с частным сектором разрешенных действий с использованием подхода, основанного на оценке риска, и разработки конкретных инструментов: процессов сертификации, руководств по передовой практике, механизмов реагирования на инциденты и, в соответствующих случаях, национальных нормативных актов.

– Эту норму не следует интерпретировать как обращенное к государству требование осуществлять упреждающий мониторинг всех ИКТ на своей территории или принимать другие превентивные меры.

ii. Государство, которому стало известно об осуществляемой с его территории вредоносной деятельности с использованием ИКТ и которое не располагает возможностями для реагирования, может принять решение обратиться за помощью к другим государствам, в том числе используя для этого типовые шаблоны запросов об оказании помощи.

– В таких случаях помощь может запрашиваться у других государств или у частных структур, а ее возможное оказание должно соответствовать национальному законодательству и международному праву в области прав человека.

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 (2015 ¶13 d)).

i. При имплементации данной нормы государствам следует:

– рассмотреть возможность оказания содействия работе Комиссии Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, в том числе путем продления мандата межправительственной группы экспертов открытого состава и поддержки ее текущих усилий по всестороннему изучению проблемы киберпреступности;

– поддерживать усилия Управления Организации Объединенных Наций по наркотикам и преступности, направленные на то, чтобы продолжать оказывать государствам-членам по их просьбе и с учетом национальных потребностей техническую помощь и содействие в деле устойчивого наращивания потенциала для борьбы с киберпреступностью по линии Глобальной программы борьбы с киберпреступностью, и в частности через ее региональные отделения, в том, что касается предотвращения, выявления, расследования и преследования в судебном порядке киберпреступности во всех ее формах, признавая, что сотрудничество с государствами-членами, компетентными международными и региональными организациями, частным сектором, гражданским обществом и другими соответствующими заинтересованными сторонами может способствовать этой деятельности;

– имплементировать уже принятые меры в соответствии с их обязательствами и рассмотреть возможность разработки новых мер, таких как принятие национальных законодательных актов по борьбе с киберпреступностью, таким образом, чтобы это соответствовало обязательствам государств в области прав человека и обеспечивало гарантии судебного характера.

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 (2015 ¶13 e))

i. Государства должны:

– выполнять свои обязательства в соответствии с национальным и международным правом при рассмотрении, разработке или имплементации национальной политики или законодательства в области кибербезопасности, а также при подготовке и реализации инициатив или создании структур, связанных с кибербезопасностью, включая меры по обеспечению защиты всех прав человека;

– при этом государствам следует учитывать мнения всех соответствующих и затронутых заинтересованных сторон на самых ранних этапах разработки и реализации политики в области кибербезопасности, с тем чтобы обеспечить комплексное рассмотрение последствий осуществления мер, связанных с кибербезопасностью;

– особенно важное значение имеет вовлечение гражданского общества с учетом его роли как одного из ключевых участников деятельности по

содействию соблюдению государством его обязательств и обязанностей в области прав человека;

– принимать во внимание, что физические лица имеют онлайн те же права, что и офлайн, и учитывать различные угрозы, с которыми могут сталкиваться женщины и представители меньшинств и уязвимых групп, в контексте прав человека;

– проводить гендерную экспертизу национальной и региональной политики в области кибербезопасности для выявления областей, в которых необходимы улучшения;

– рассмотреть вопрос о включении мер по устранению последствий ИКТ для прав человека в свои национальные планы действий в области предпринимательства и прав человека.

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 (2015 ¶13 f)).

i. Каждое государство определяет, какие инфраструктуры или сектора оно считает критическими, в соответствии с национальными приоритетами и способами классификации критической инфраструктуры. К секторам критической инфраструктуры, которые используются для оказания населению базовых услуг, могут относиться, в частности, энергетика, водоснабжение, водоотведение, здравоохранение, образование, финансы, транспорт, телекоммуникации и структуры реагирования на кризисные ситуации. К критической инфраструктуре может также относиться техническая инфраструктура, необходимая для проведения выборов, референдумов или плебисцитов, и техническая инфраструктура, необходимая для обеспечения общедоступности и надежности Интернета. Упоминание такой инфраструктуры в качестве примеров ни в коей мере не препятствует определению государствами в качестве критической других видов инфраструктуры и не означает косвенного попустительства в отношении злонамеренных действий против какой-либо категории, критической инфраструктуры, не указанной выше.

ii. Государства должны учитывать потенциально вредоносные последствия своей деятельности в области ИКТ для технической инфраструктуры, имеющей важное значение для общедоступности и надежности Интернета.

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 (2015 ¶13 g)).

i. В целях содействия формированию глобальной культуры кибербезопасности государствам следует рассматривать в соответствующих случаях возможность обмена информацией о передовой практике в области защиты критической инфраструктуры, включая все элементы, указанные в этой резолюции, а также о:

– основных требованиях в сфере безопасности;

– процедурах уведомления об инцидентах;

– инструментах и методах реагирования на инциденты;

– устойчивости в случае чрезвычайных ситуаций;

– выводах, сделанных по итогам предыдущих инцидентов.

ii. Наращивание потенциала и другие меры по формированию глобальной культуры кибербезопасности должны разрабатываться на основе широкого участия и учитывать гендерные аспекты кибербезопасности.

iii. Ввиду разнообразия и распределенного характера форм собственности, в которой могут находиться объекты критической инфраструктуры, государствам следует надлежащим образом и в консультации с соответствующими заинтересованными сторонами содействовать соблюдению минимальных стандартов безопасности критической инфраструктуры и поощрять сотрудничество с частным сектором, научными кругами и техническим сообществом в рамках усилий по защите критической инфраструктуры.

iv. Государства должны соответствующим образом участвовать в добровольных инициативах по оценке рисков и планированию мероприятий по обеспечению бесперебойной деятельности (устойчивость, восстановление и реагирование на экстренные ситуации), в которых участвуют и другие заинтересованные стороны и которые направлены на повышение безопасности и устойчивости объектов критической инфраструктуры, оказывающих услуги на региональном или международном уровне, перед лицом существующих и возникающих угроз.

v. Усилия по защите критической информационной инфраструктуры следует предпринимать с должным учетом применимого национального законодательства в сфере защиты частной жизни и другого соответствующего законодательства.

vi. При подготовке указаний относительно имплементации норм f) и g) государства учитывают, что выделение определенных секторов в качестве критической инфраструктуры не предполагает составления исчерпывающего перечня и не влияет на определение государством какого-либо другого сектора в качестве критически важного, а также не означает косвенного попустительства в отношении злонамеренных действий против какой-либо категории, не включенной в такой перечень.

vii. РГОС подчеркнула, что все государства рассматривают инфраструктуру системы здравоохранения, медицинские службы и медицинские учреждения в качестве критической инфраструктуры для целей норм f) и g). С учетом того, что РГОС вела подготовку своего доклада в условиях пандемии COVID-19, необходимость подтверждения того, что инфраструктура систем здравоохранения нуждается в защите, ощущалась особенно остро.

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 также должны 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 (2015 ¶13 h)).

i. Имплементация данной нормы предполагает рассмотрение соответствующих просьб об оказании помощи и учет характера помощи, которая может быть своевременно предложена. Государства, получающие соответствующую просьбу об оказании помощи после инцидента в сфере ИКТ, должны, когда это возможно, целесообразно и допустимо, сделать следующее:

– подтвердить получение просьбы через соответствующий национальный контактный пункт;

– оперативно определить, располагают ли они возможностями и ресурсами для оказания запрашиваемой помощи. Для этого может потребоваться уточнение у ряда заинтересованных сторон информации об имеющихся экспертных возможностях;

– указать в своем первоначальном ответе характер, объем и условия оказания помощи, которая может быть предоставлена, включая сроки ее предоставления;

– в случае, если оказание помощи согласовано, оперативно обеспечить ее предоставление;

– обеспечивать, чтобы просьбы об оказании помощи, включая соответствующие процессы и ресурсы, такие как рамки и шаблоны, а также ответы на них соответствовали обязательствам в области прав человека.

ii. Имплементации данной нормы дополнительно способствовали бы заблаговременное создание национальных структур и механизмов, включая национальный контактный пункт, шаблоны просьб об оказании помощи и подтверждений готовности оказать такую помощь, а также целенаправленное наращивание потенциала и оказание технической помощи. Определенную роль в содействии их развитию могут играть инициативы в области двустороннего и многостороннего сотрудничества, международные и региональные организации и форумы.

Положительный вклад в имплементацию данной нормы могли бы внести, в частности, следующие подходы: расширение сотрудничества на национальном и международном уровнях между государственными учреждениями, частным сектором и организациями гражданского общества, особенно в области принятия превентивных мер; наращивание потенциала групп реагирования на инциденты на основе адресного подхода к развитию киберпотенциала; и специализированная подготовка в целях наращивания киберпотенциала на всех уровнях государства и в обществе в целом.

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 скрытых вредоносных функций (2015 ¶13 i)).

i. Для имплементации данной нормы государства должны:

– предпринимать шаги, в том числе через существующие площадки, для предотвращения распространения злонамеренных программных и технических средств в сфере ИКТ. При этом государствам следует поощрять законную деятельность по обеспечению безопасности систем ИКТ, ведущуюся исследовательскими сообществами, научными кругами, промышленными предприятиями, правоохранительными органами, CERTs/CSIRTs и другими учреждениями, занимающимися вопросами кибербезопасности;

– рассмотреть вопрос об обмене информацией о факторах уязвимости в сфере ИКТ и/или скрытых вредоносных функциях в ИКТ-продуктах;

– заниматься внедрением средств контроля безопасности, основанных на управлении рисками.

j. Государства должны способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться 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 (2015 ¶13 j)).

i. Для имплементации данной нормы государства должны:

– создавать национальные структуры, обеспечивающие ответственное представление информации о факторах уязвимости в сфере ИКТ и их устранение;

– содействовать созданию механизмов координации между субъектами государственного и частного секторов.

ii. Кроме того, во избежание недопонимания или неправильного толкования, в том числе по причине нераскрытия информации о потенциально вредоносных факторах уязвимости в сфере ИКТ, государствам рекомендуется как можно шире делиться, когда это целесообразно, технической информацией о серьезных инцидентах в сфере ИКТ, используя существующие механизмы координации работы различных CERT, а также механизмы, созданные региональными организациями (такие, как сети контактных пунктов). Государствам следует обеспечивать, чтобы такая информация обрабатывалась ответственно и при необходимости в координации с другими заинтересованными сторонами.

k. Государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным инцидентам (также именуемым группами готовности к компьютерным инцидентам или группами готовности к инцидентам в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности (2015 ¶13 k)).

Китай

- Государства должны взять на себя обязательство не использовать ИКТ и ИКТ-сети для осуществления деятельности, которая противоречит задаче поддержания международного мира и безопасности.

Государственный суверенитет в киберпространстве

- Государства должны обладать на своей территории юрисдикцией над ИКТ-инфраструктурой и ИКТ-ресурсами, а также над деятельностью, связанной с использованием ИКТ.
- Государства имеют право проводить государственную политику в сфере ИКТ сообразно национальным условиям для распоряжения собственными делами в сфере ИКТ и защиты законных интересов своих граждан в киберпространстве.
- Государства должны воздерживаться от использования ИКТ для вмешательства во внутренние дела других государств и подрыва их политической, экономической и социальной стабильности.
- Государства должны на равноправной основе участвовать в распоряжении международными интернет-ресурсами и их распределении.

Защита критической инфраструктуры

- Государства имеют права и обязанности в отношении правовой защиты своей критической ИКТ-инфраструктуры от ущерба, причиняемого в результате угроз, вмешательства, нападений и саботажа.
- Государства должны воздерживаться от кибератак на критическую инфраструктуру других государств.
- Государства не должны использовать политические и технические преимущества для подрыва безопасности и целостности критической инфраструктуры других государств.
- Государства должны расширять обмен информацией о стандартах и передовой практике в области защиты критической инфраструктуры и поощрять предприятия к участию в таком обмене.

Безопасность данных

- Государства должны придерживаться сбалансированного подхода в отношении технического прогресса, развития предпринимательства и защиты национальной безопасности и общественных интересов.
- Государства имеют права и обязанности по обеспечению безопасности личной информации и важных данных, имеющих отношение к их национальной безопасности, общественной безопасности, экономической безопасности и социальной стабильности.
- Государства не должны осуществлять или поддерживать шпионаж с использованием ИКТ против других государств, включая массовую слежку и хищение важных данных и личной информации.
- Государства должны уделять равное внимание как развитию, так и безопасности и добиваться законной, упорядоченной и свободной передачи данных. Государства должны содействовать обмену передовым опытом и сотрудничеству в этой области.

Безопасность цепочек поставок

- Государства не должны использовать свое доминирующее положение в сфере ИКТ, в том числе превосходство в ресурсах, критической ИКТ-инфраструктуре и ключевых технологиях, товарах и услугах в сфере ИКТ, для ущемления права других государств на независимый контроль над товарами и услугами в сфере ИКТ и подрыва их безопасности.
- Государства должны запретить поставщикам товаров и услуг в сфере ИКТ незаконно получать данные пользователей, контролировать пользовательские устройства и системы и манипулировать ими путем установки в продуктах программных закладок. Государства должны также запретить поставщикам товаров и услуг в сфере ИКТ преследовать свои незаконные интересы, пользуясь зависимостью пользователей от их продукции или вынуждая пользователей обновлять свои системы или устройства. Государства должны обратиться к поставщикам товаров и услуг в сфере ИКТ с просьбой взять на себя обязательство своевременно уведомлять своих партнеров по сотрудничеству и пользователей в случае обнаружения в их продуктах серьезных факторов уязвимости.
- Государства должны быть привержены поддержанию справедливой, равноправной и недискриминационной деловой среды. Государства не должны использовать национальную безопасность в качестве предлога для ограничения развития и сотрудничества в сфере ИКТ и ограничения доступа на рынки ИКТ-продукции и экспорта высокотехнологичной продукции.

Борьба с терроризмом

- Государства должны запретить террористическим организациям использовать Интернет для создания веб-сайтов, онлайн-форумов и блогов для осуществления террористической деятельности, включая изготовление, публикацию, хранение и трансляцию аудио- и видеоматериалов террористического характера, распространение агрессивной террористической риторики и идеологии, сбор средств, вербовку, подстрекательство к террористической деятельности и т.д.

- Государства должны осуществлять обмен разведывательными данными и поддерживать сотрудничество между правоохранительными органами в сфере борьбы с терроризмом. Например, в случае поступления от других государств запроса по делам, связанным с террористической деятельностью в киберпространстве, получившее такой запрос государство должно обеспечить оперативный сбор в сети Интернет и хранение соответствующих данных и доказательств, оказать помощь в проведении расследования и оперативно отреагировать на запрос.

- Государства должны развивать партнерские отношения сотрудничества с международными организациями, предприятиями и гражданами в борьбе с кибертерроризмом.

- Государства должны обращаться к поставщикам интернет-услуг с просьбами перекрыть онлайновые каналы распространения материалов террористической направленности, блокируя веб-сайты и учетные записи, с которых ведется пропаганда, и удаляя материалы террористического и экстремистского толка, содержащие призывы к насилию.

Словения, Финляндия, Франция и Хорватия

- Следует рекомендовать государствам принимать меры с целью воспрепятствовать осуществлению негосударственными субъектами, включая частный сектор, деятельности в сфере ИКТ в своих собственных целях или в целях других негосударственных субъектов в ущерб третьим сторонам, в том числе находящимся на территории другого государства.

- Эта цель может быть достигнута благодаря определению во взаимодействии с частным сектором допустимых действий с использованием подхода, основанного на оценке риска, и разработке конкретных инструментов: процессов сертификации, руководств по передовой практике, механизмов реагирования на инциденты и при необходимости национальных нормативных актов.

Куба

Сложившаяся ситуация требует имплементации конкретных положений, дополняющих международное право и направленных, в частности, на решение следующих столь же важных задач:

- предотвращение применения односторонних мер и направленных против государств мер, препятствующих всеобщему доступу к преимуществам от использования ИКТ;

- смягчение пагубных последствий присвоения ответственности в контексте кибератак;

- предотвращение милитаризации киберпространства;

- обеспечение более эффективной защиты личных данных граждан посредством содействия принятию в этой сфере международных норм;

- дополнение законодательства о кибертерроризме в целях противодействия инцидентам и проблемам, связанным с кибербезопасностью, таким как кибератаки. Выработка единой позиции в отношении того, что понимается под кибератакой;

- более объективное практическое применение принципов международного права в этой области.

Чешская Республика

- Государства не должны осуществлять или сознательно поддерживать деятельность в киберпространстве, которая может нанести ущерб медицинским службам или медицинским учреждениям, и должны принимать меры по защите медицинских служб от вреда[14].
- Необходимо соблюдать существующие обязательства по международному праву в области прав человека при рассмотрении, разработке и проведении национальной политики и применении законодательства в области кибербезопасности[15].
- Необходимо учитывать мнения всех соответствующих и затронутых заинтересованных сторон на самом раннем этапе разработки политики в области кибербезопасности для обеспечения всестороннего рассмотрения последствий принятия мер по обеспечению кибербезопасности для прав человека[16].

Эквадор

- Указание по имплементации нормы 13 b) (доклад ГПЭ 2015 года)[17]:

i) государства могли бы создать национальные структуры и координационные механизмы, а также разработать стратегии и процессы, необходимые для содействия тщательному рассмотрению серьезных инцидентов в сфере ИКТ и определения надлежащих мер реагирования;

ii) затем государства могли бы разработать шаблоны для описания инцидентов в сфере ИКТ или степени их серьезности для подготовки предварительной и окончательной оценок инцидентов в сфере ИКТ;

iii) обеспечение прозрачности таких шаблонов и их согласование региональными организациями могли бы обеспечить общность подходов государств к рассмотрению инцидентов в сфере ИКТ и улучшить коммуникацию между государствами;

iv) при рассмотрении всей значимой информации, касающейся инцидента в сфере ИКТ, государствам следует изучать возможные гендерно-дифференцированные последствия и проводить совместную работу со всеми заинтересованными сторонами, с тем чтобы понять более общий контекст инцидента в сфере ИКТ, включая его влияние на осуществление прав женщин.

[14] URL: https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-buildinternational-law.

[15] URL: https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber- Security-07.02.pdf.

[16] URL: https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber- Security-07.02.pdf.

[17] 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.

• Предлагаются следующие указания по имплементации нормы 13 c)[18]:

i) если государство выявляет злонамеренную активность с использованием киберсредств, исходящую с территории или с использованием киберинфраструктуры другого государства, то первым шагом может стать направление этому государству соответствующего уведомления. Ключевую роль в выявлении такой активности играют группы реагирования на компьютерные инциденты;

ii) с учетом того, что инциденты в сфере ИКТ могут совершаться с территории третьих государств или при их участии, следует понимать, что направление уведомления тому или иному государства не означает возложения на это государство ответственности за инцидент;

iii) получившее уведомление государство должно подтвердить получение запроса через соответствующий национальный контактный пункт;

iv) когда государству известно, что его территория или киберинфраструктура используется для осуществления противоправных действий международного характера с использованием ИКТ, которые могут привести к серьезным неблагоприятным последствиям в другом государстве, первому государству следует попытаться принять разумные, доступные и практически осуществимые меры в пределах своей территории и возможностей в соответствии со своими обязательствами согласно внутреннему и международному праву, с тем чтобы пресечь такие противоправные действия международного характера или смягчить их последствия;

v) эту норму не следует интерпретировать как обращенное к государству требование осуществлять упреждающий мониторинг всех ИКТ на своей территории или принимать другие превентивные меры;

vi) государство, которому стало известно об осуществляемой с его территории вредоносной деятельности с использованием ИКТ и которое не располагает возможностями для реагирования, может принять решение обратиться за помощью к другим государствам, в том числе используя для этого типовые шаблоны запросов об оказании помощи;

vii) В таких случаях помощь может запрашиваться у других государств или у частных структур в порядке, соответствующем национальному законодательству. Важное значение в этой связи имеет приверженность государств сотрудничеству с другими странами и оказанию им помощи в случае кризиса; при этом следует особо учитывать, что инциденты в сфере ИКТ могут оказывать дифференцированное влияние на конкретные инфраструктуры в развивающихся странах.

• В проект следует также включить новые нормы, в том числе следующую:

«Государства не должны осуществлять операции с использованием ИКТ, направленные на нарушение функционирования технической инфраструктуры, необходимой для осуществления политических процессов, таких как выборы, референдумы или плебисциты».

[18] Государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ.

Индия

- (Относительно пункта 39): Предлагается разработать новую норму касательно необходимости принятия согласованного стандарта основных параметров безопасности в киберпространстве в отношении наиболее эффективных способов оптимизации использования перспективных технологий при одновременной защите интересов общества. Для этого государства должны решительно поддержать повсеместное принятие и верифицируемую имплементацию основных правил кибергигиены.

- Защита критической информационной инфраструктуры является одним из элементов ответственного поведения государств. Угроза критической информационной инфраструктуре может нарушить целостность информации и навредить экономике и экономическому развитию страны. Государства должны рассмотреть вопрос о защите КИИ в рамках государственно-частного партнерства. Государства не должны проводить операции с использованием ИКТ, направленные на нарушение функционирования КИИ. Государства не должны закладывать вредоносные функции в ИКТ-продукты. Государства должны нести ответственность за уведомление пользователей при выявлении существенных факторов уязвимости и уведомление поставщиков о необходимости устранения таких факторов уязвимости. Государства должны сотрудничать в сфере КИИ, обмениваться информацией об угрозах и делиться инструментами и методами, позволяющими смягчить их последствия.

Исламская Республика Иран

- Следует повысить роль государств, несущих главную ответственность за поддержание безопасной, надежной и заслуживающей доверия ИКТ-среды, в регулировании ИКТ-среды, включая определение политики и выработку решений на глобальном уровне. Подобное регулирование ИКТ-среды должно осуществляться таким образом, чтобы укреплять государственный суверенитет и не ущемлять права государств при выборе ими моделей развития, управления и законодательства в ИКТ-среде.

- Государства должны воздерживаться от угрозы силой или ее применения против территориальной целостности или политической независимости любого государства в рамках и посредством ИКТ-среды.

- Ни одно государство не имеет права вмешиваться прямо или косвенно с использованием средств и методов, связанных с ИКТ, по какой бы то ни было причине во внутренние и внешние дела других государств. Любые формы вмешательства и воздействия и всякие угрозы, направленные против политических, экономических, социальных и культурных систем, а также против связанной с киберпространством критической информационной инфраструктуры государств, должны осуждаться и пресекаться (резолюция 2131 Генеральной Ассамблеи Организации Объединенных Наций от 21 декабря 1965 года).

- Государства не должны использовать достижения в сфере ИКТ в качестве инструментов экономического, политического или любого иного принуждения, включая меры ограничения или блокировки, против определенных государств (резолюция 2131 Генеральной Ассамблеи Организации Объединенных Наций от 21 декабря 1965 года).

- Государства должны обеспечивать принятие надлежащих мер, с тем чтобы предприятия частного сектора, деятельность которых имеет экстерриториальные последствия, включая платформы, несли ответственность за свое поведение в ИКТ-среде. Государства должны осуществлять надлежащий контроль над ИКТ-компаниями и платформами, находящимися под их юрисдикцией, в противном случае они несут ответственность за сознательное нарушение национального суверенитета, безопасности и общественного порядка других государств.
- Государства должны воздерживаться от злоупотреблений сформировавшимися под их контролем и в рамках их юрисдикции каналов поставки ИКТ-продукции в целях создания или содействия возникновению факторов уязвимости в продуктах, услугах и техническом обслуживании, ставящих под угрозу суверенитет и сохранность данных определенных государств, и пресекать такие злоупотребления.

Япония

Новое предложение, которое Япония представляет на рассмотрение РГОС, заключается в добавлении следующей формулировки в качестве указания по имплементации нормы i) по обеспечению целостности каналов поставки:

- «Государства имеют право и несут обязанность обеспечивать использование проверенных поставщиков и продавцов оборудования и систем ИКТ, в особенности с учетом соображений национальной безопасности и для защиты личной информации. Разумные шаги могут включать принятие законодательных или административных мер для обеспечения безопасности каналов поставки, содействия разработке надежных и заслуживающих доверия технологий и промышленных решений и диверсификации поставщиков».

Нидерланды

- «Государственные и негосударственные субъекты не должны осуществлять или заведомо допускать деятельность, которая преднамеренно и существенно подрывает общедоступность или целостность опорных сетей Интернета и, следовательно, стабильность киберпространства» — [такая формулировка могла бы использоваться как] указание по имплементации рекомендации 13 f), содержащейся в докладе ГПЭ 2015 года, которое при этом затрагивает рекомендацию 13 g), содержащуюся в докладе ГПЭ 2015 года.
- «Государственные и негосударственные субъекты не должны осуществлять, поддерживать или допускать кибероперации в целях нарушения функционирования технической инфраструктуры, необходимой для проведения выборов, референдумов или плебисцитов» — [такая формулировка могла бы использоваться как] указание по имплементации рекомендации 13 f), содержащейся в докладе ГПЭ 2015 года, которое при этом затрагивает рекомендацию 13 g), содержащуюся в докладе ГПЭ 2015 года.

Движение неприсоединения

- Следует рекомендовать государствам-членам собирать и систематизировать информацию об имплементации ими международных норм, которую они должны представлять, и о соответствующей предлагаемой базе данных

для хранения данной информации в целях регулирования конкретных аспектов использования ИКТ государствами с точки зрения международной безопасности и выявления областей, которые вызывают взаимную озабоченность.

- Государства-члены не должны осуществлять и заведомо поддерживать никакую деятельность в сфере ИКТ, которая в нарушение норм международного права наносит преднамеренный ущерб или препятствует использованию и функционированию критически важной инфраструктуры других государств-членов.
- Следует настоятельно призвать государства-члены рассмотреть вопрос об обмене информацией о факторах уязвимости ИКТ и/или скрытых вредоносных функциях в ИКТ-продуктах, а также призвать их уведомлять пользователей в случае выявления существенных факторов уязвимости.
- Государства-члены должны также принимать во внимание резолюцию 73/27 Генеральной Ассамблеи Организации Объединенных Наций при осуществлении любой деятельности, связанной с ИКТ.
- Движение неприсоединения вновь заявляет о своей глубокой обеспокоенности по поводу все более широкого применения одностороннего подхода и в этой связи подчеркивает, что единственным надежным способом решения вопросов международной безопасности являются многосторонний подход и согласование решений в многостороннем формате в соответствии с Уставом Организации Объединенных Наций.
- Движение неприсоединения вновь заявляет о том, что все государства должны воздерживаться от угрозы силой или ее применения против территориальной целостности или политической независимости любого государства в рамках и посредством ИКТ-среды.
- Движение неприсоединения призывает активизировать усилия, направленные на недопущение превращения киберпространства в арену конфликтов и на обеспечение его использования исключительно в мирных целях, что позволило бы в полной мере реализовать потенциал ИКТ для содействия социально-экономическому развитию.
- Движение неприсоединения обращает особое внимание на важность недопущения введения неоправданных ограничений, в том числе посредством принятия односторонних принудительных мер, на использование ИКТ в мирных целях, международное сотрудничество или передачу технологий.
- Движение неприсоединения особо отмечает, что государства несут главную ответственность за поддержание открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.
- Движение неприсоединения подчеркивает, что ни одно 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 .

Пакистан

- Следует рекомендовать государствам-членам продолжить рассмотрение в соответствующем порядке возможности принятия юридически и/или политически обязывающего инструмента(-ов) для регулирования конкретных аспектов использования ИКТ государствами в контексте международной безопасности.
- Следует рекомендовать государствам-членам выработать согласованное общее определение «критически важной инфраструктуры», с тем чтобы договориться о запрещении деятельности в сфере ИКТ, которая наносит заведомый и преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры.
- Следует рекомендовать государствам-членам сотрудничать в целях достижения договоренности о запрещении создания скрытых вредоносных функций или накопления в продуктах ИКТ факторов уязвимости, а также взять на себя обязательство ответственно и своевременно представлять информацию о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих способах устранения таких факторов уязвимости.
- Государства-члены должны стремиться содействовать сотрудничеству с поставщиками товаров и услуг в сфере ИКТ, с тем чтобы предотвратить недобросовестное использование ими личных данных пользователей или сведений о частной жизни и злоупотребление такими данными и сведениями.
- Государства-члены должны взять на себя обязательство не использовать ИКТ для осуществления деятельности, противоречащей задаче поддержания международного мира и безопасности, и воздерживаться от использования ИКТ для вмешательства каким-либо образом во внутренние дела других государств.
- Государства-члены должны сотрудничать в целях решения проблем, связанных с присвоением ответственности в ИКТ-среде. Разработка общего подхода к присвоению ответственности в рамках универсальной процедуры под эгидой Организации Объединенных Наций остается наиболее эффективным способом продвижения вперед в этом направлении.
- Следует настоятельно призвать государства-члены прийти к соглашению о запрещении деятельности в сфере ИКТ, направленной на нарушение функционирования технической инфраструктуры, необходимой для проведения выборов, референдумов или плебисцитов.
- Следует рекомендовать государствам-членам разрабатывать и имплементировать нормы таким образом, чтобы избегать введения неоправданных ограничений на использование ИКТ в мирных целях, международное сотрудничество в этой области или передачу технологий.

Республика Корея

Предлагаемое указание по имплементации пункта 13 c) доклада ГПЭ 2015 года:

- Когда затронутое государство уведомляет другое государство о том, что инциденты в сфере ИКТ были совершены с территории уведомляемого

государства или при его участии, и сопровождает это проверенной информацией, получившее уведомление государство должно принять все разумные меры в пределах своей территории и возможностей согласно международному и внутреннему праву, с тем чтобы пресечь эту деятельность или смягчить ее последствия.

- Следует понимать, что такое уведомление не означает возложения на получившего его государство ответственности за инцидент.
- В качестве минимального требования к проверенной информации можно установить, в частности, наличие индикаторов компрометации, таких как IP-адрес, местонахождение нарушителей и компьютеров, использованных для злонамеренных действий в сфере ИКТ, и данные о вредоносных программах.