Организация Объединенных Наций A/78/265

Генеральная Ассамблея

Distr.: Limited
1 August 2023
Russian
Original: English

**Семьдесят восьмая сессия**
Пункт 96 предварительной 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 второй ежегодный доклад о проделанной работе, представленный Рабочей группой открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025.

* A/78/150.

23-14962 (R) 130923 180923

# Доклад Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025

## I. Введение

1. В своей резолюции 75/240 Генеральная Ассамблея постановила созвать, начиная с 2021 года, в целях обеспечения непрерывности и преемственности демократического, инклюзивного и транспарентного переговорного процесса по безопасности в сфере использования информационно-коммуникационных технологий под эгидой Организации Объединенных Наций новую рабочую группу открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, действующую на основе консенсуса, в целях продолжения в качестве приоритета дальнейшей выработки норм, правил и принципов ответственного поведения государств и путей их имплементации, при необходимости, внесения в них изменений или формулирования дополнительных правил поведения; рассмотрения инициатив государств, направленных на обеспечение безопасности в сфере использования ИКТ; организации под эгидой Организации Объединенных Наций регулярного институционального диалога с широким кругом государств-участников; а также продолжения в целях выработки общего понимания исследования существующих и потенциальных угроз в сфере информационной безопасности, в том числе безопасности данных, и возможных совместных мер по их предотвращению и противодействию им и того, как международное право применяется к использованию ИКТ государствами, мер укрепления доверия и наращивания потенциала; и представления ежегодных промежуточных докладов о проделанной работе и итогового доклада, принимаемых консенсусом, о результатах своей деятельности Ассамблее на ее восьмидесятой сессии.

2. Первый ежегодный доклад Рабочей группы о проделанной работе, посвященный ее организационной сессии и ее первой, второй и третьей основным сессиям, был опубликован в виде документа A/77/275.

## II. Организационные вопросы

### A. Открытие и продолжительность четвертой и пятой основных сессий

3. Рабочая группа провела свою четвертую основную сессию 6–10 марта 2023 года и свою пятую основную сессию 24–28 июля 2023 года в Центральных учреждениях Организации Объединенных Наций.

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 четвертой и пятой основных сессий приводится в документах A/AC.292/2023/INF/2 и A/AC.292/2023/INF/4 соответственно.

## C. Должностные лица

6. На своих четвертой и пятой основных сессиях рабочая группа действовала под председательством г-на Бурхана Гафура (Сингапур).

## D. Организация работы

7. На 1-м заседании четвертой основной сессии, состоявшемся 6 марта 2023 года, рабочая группа утвердила порядок организации своей работы, изложенный в документе A/AC.292/2023/2/Rev.1. Она также одобрила участие в ее работе неправительственных структур, перечисленных в документе A/AC.292/2023/INF/1.

8. На 1-м заседании пятой основной сессии, состоявшемся 24 июля 2023 года, Рабочая группа утвердила порядок организации своей работы, изложенный в документе A/AC.292/2023/3. Она также одобрила участие в ее работе неправительственных структур, перечисленных в документе A/AC.292/2023/INF/3.

## E. Документация

9. С полным перечнем всех официальных, рабочих, технических и других документов, имевшихся в распоряжении Рабочей группы, можно ознакомиться на специальном веб-сайте (https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021).

## F. Деятельность Рабочей группы

10. На своей четвертой основной сессии в ходе 10 пленарных заседаний рабочая группа рассмотрела пункты 3, 5 и 6 повестки дня.

11. На своей пятой основной сессии в ходе 10 пленарных заседаний Рабочая группа рассмотрела пункты 3 и 5–7 повестки дня.

12. 5–9 декабря 2022 года, 2 марта 2023 года и 23–26 мая 2023 года Председатель, руководствуясь решением 77/512 Генеральной Ассамблеи, созывал межсессионные совещания для выслушивания мнений по рассматриваемым рабочей группой темам, которые указаны в мандате Рабочей группы, изложенном в резолюции 75/240 Ассамблеи, и в повестке дня Рабочей группы (A/AC.292/2021/1).

13. 9 марта и 26 июля 2023 года в соответствии с согласованным порядком участия заинтересованных сторон в ходе 8-го заседания четвертой основной сессии и 5-го заседания пятой основной сессии были проведены специальные заседания заинтересованных сторон.

14. 1 марта, 22 мая и 11 июля 2023 года Председатель провел неофициальные консультативные обсуждения с заинтересованными сторонами, включая представителей деловых кругов, неправительственных структур и научно-академического сообщества, чтобы выслушать мнения по рассматриваемым Рабочей группой открытого состава темам, которые указаны в мандате Рабочей группы, изложенном в резолюции 75/240 Генеральной Ассамблеи, и в повестке дня Рабочей группы (A/AC.292/2021/1), а также конкретные идеи, которые Рабочая группа могла бы рассмотреть в дальнейшем.

# III. Утверждение доклада

15. На своей пятой основной сессии Рабочая группа рассмотрела 28 июля 2023 года пункт 7 повестки дня, озаглавленный «Утверждение ежегодных докладов о проделанной работе», и утвердила проект доклада Рабочей группы открытого состава (A/AC.292/2023/L.1). Она также постановила включить в свой доклад итоги состоявшихся в Рабочей группе обсуждений по пункту 5 повестки дня, изложенные в документе A/AC.292/2023/CRP.1 с внесенными в него устными изменениями (см. приложение).

16. Подборка заявлений с разъяснением позиций будет издана в качестве документа A/AC.292/2023/INF/5.

# Приложение*

## Доклад о ходе обсуждения Рабочей группой пункта 5 повестки дня

### A. Общий обзор

1. Четвертая и пятая официальные сессии, а также неофициальные межсессионные совещания Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ 2021–2025 проходили во все столь же сложной геополитической обстановке, характеризующейся нарастающей обеспокоенностью по поводу злонамеренного использования ИКТ государственными и негосударственными субъектами, которая влияет на международный мир и безопасность.

2. В ходе этих сессий государства сослались на консенсусные решения и резолюции Генеральной Ассамблеи, в которых государства согласились руководствоваться при использовании ИКТ докладами РГОС и Группы правительственных экспертов (ГПЭ)[1]. В этой связи государства также напомнили о результатах работы первой РГОС, которая была учреждена резолюцией 73/27 Генеральной Ассамблеи и завершила свою работу в 2021 году, представив свой заключительный доклад, согласованный на основе консенсуса[2], а также приняли к сведению резюме Председателя и неисчерпывающий перечень предложений, содержащийся в приложении к резюме Председателя, и напомнили о результатах работы шестой ГПЭ, которая была учреждена резолюцией 73/266 Генеральной Ассамблеи и завершила свою работу в 2021 году, представив свой заключительный доклад, согласованный на основе консенсуса[3].

3. Кроме того, государства вновь подтвердили первый ежегодный доклад нынешней РГОС о проделанной работе[4], консенсусный доклад РГОС 2021 года о достижениях в сфере ИКТ в контексте международной безопасности и консенсусные доклады ГПЭ 2010, 2013, 2015 и 2021 годов[5]. Государства напомнили и подтвердили, что в этих докладах группы «рекомендовали 11 добровольных, не имеющих обязательной силы норм ответственного поведения государств и признали, что со временем могут быть разработаны дополнительные нормы» и что «в них содержались рекомендации в отношении конкретных мер в области укрепления доверия, наращивания потенциала и сотрудничества». Государства также напомнили и подтвердили, что «международное право, в частности Устав Организации Объединенных Наций, применимо и необходимо для поддержания мира, безопасности и стабильности в ИКТ-среде»[6]. Эти элементы укрепляют кумулятивные и эволюционирующие рамки ответственного поведения государств в области использования ИКТ[7], ложась в основу работы нынешней РГОС.

---

* Публикуется без официального редактирования.

[1] Решения 75/564 и 77/512 и резолюции 70/237 и 76/19 Генеральной Ассамблеи.

[2] A/75/816.

[3] A/76/135.

[4] A/77/275.

[5] A/65/201, A/68/98, A/70/174 и A/76/135.

[6] Доклад РГОС 2021 года (A/75/816), приложение I, пункт 7.

[7] Доклад ГПЭ 2021 года (A/76/135), пункт 2; принятая на основе консенсуса резолюция 76/19 Генеральной Ассамблеи.

4. РГОС сослалась на свой мандат, который содержится в резолюции 75/240 Генеральной Ассамблеи и сформулирован следующим образом: «... действующую на основе консенсуса, в целях продолжения в качестве приоритета дальнейшей выработки норм, правил и принципов ответственного поведения государств и путей их имплементации, при необходимости, внесения в них изменений или формулирования дополнительных правил поведения; рассмотрения инициатив государств, направленных на обеспечение безопасности в сфере использования ИКТ; организации под эгидой Организации Объединенных Наций регулярного институционального диалога с широким кругом государств-участников; а также продолжения в целях выработки общего понимания исследования существующих и потенциальных угроз в сфере информационной безопасности, в том числе безопасности данных, и возможных совместных мер по их предотвращению и противодействию им, и того, как международное право применяется к использованию ИКТ государствами, мер укрепления доверия и наращивания потенциала; и представления ежегодных промежуточных докладов о проделанной работе и итогового доклада, принимаемых консенсусом, о результатах своей деятельности Генеральной Ассамблее на ее восьмидесятой сессии». В этой связи РГОС признала важность сбалансированного выполнения своего мандата и необходимость уделить должное внимание как дальнейшему содействию достижению государствами общего понимания в вопросах безопасности в сфере использования ИКТ, так и дальнейшему выполнению существующих обязательств.

5. РГОС признала, что наращивание потенциала является важной мерой укрепления доверия, что эта тема затрагивает все основные направления работы РГОС и что целостный подход к наращиванию потенциала в контексте безопасности ИКТ крайне важен. В связи с этим возникает необходимость в разработке устойчивых, эффективных и доступных решений.

6. РГОС привержена взаимодействию с заинтересованными сторонами на систематической, устойчивой и содержательной основе в порядке, согласованном в соответствии с процедурой молчания 22 апреля 2022 года и официально утвержденном на первом заседании третьей сессии РГОС 25 июля 2022 года, и сообразно своему мандату, который содержится в резолюции 75/240 Генеральной Ассамблеи и предусматривает взаимодействие, при необходимости, с другими заинтересованными сторонами, включая представителей деловых кругов, неправительственных организаций и научно-академического сообщества.

7. РГОС признала, что региональные и субрегиональные организации могут продолжать играть важную роль в применении рамок ответственного поведения государств в области использования ИКТ. Кроме того, региональные, межрегиональные и межорганизационные обмены могут способствовать созданию новых возможностей для сотрудничества, взаимодействия и взаимного обучения. Поскольку не все государства являются членами той или иной региональной организации и не все региональные организации уделяют внимание вопросам безопасности в сфере использования ИКТ, РГОС отметила, что предпринимаемые на региональном уровне усилия служат дополнением к ее работе.

8. РГОС приветствовала высокий уровень участия женщин-делегатов в работе ее сессий и то большое внимание, которое уделяется в ее обсуждениях гендерным аспектам. РГОС подчеркнула важность сокращения «гендерного цифрового разрыва» и содействия полному, равноправному и значимому участию и лидерству женщин в процессах принятия решений, связанных с использованием ИКТ в контексте международной безопасности.

9. Данный второй ежегодный доклад о проделанной работе содержит информацию о конкретных действиях и совместных мерах по противодействию угрозам в сфере ИКТ и содействию создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды и в этом отношении опирается на первый ежегодный доклад о проделанной работе (A/77/275), одобренный консенсусом в решении 77/512 Генеральной Ассамблеи. В знак признания того, что в РГОС ведутся непрерывные обсуждения и что обсуждения по существу в ходе работы РГОС будут проводиться до завершения ее мандата в 2025 году, настоящий второй ежегодный доклад о проделанной Группой работе не преследует цели дать всеобъемлющее резюме ведущихся государствами обсуждений, а призван отразить конкретный прогресс, достигнутый РГОС на сегодняшний день, опираясь также на «дорожную карту» для проведения обсуждений, изложенную в первом ежегодном докладе о проделанной работе. Этот второй ежегодный доклад о проделанной работе будет представлен Генеральной Ассамблее в соответствии с мандатом РГОС, содержащимся в резолюции 75/240.

## B. Существующие и потенциальные угрозы

10. В ходе четвертой, пятой, а также неофициальных сессий РГОС государства продолжили обсуждение существующих и потенциальных угроз. В этой связи государства напомнили о том, что сфера деятельности РГОС включает рассмотрение угроз в сфере ИКТ в контексте международной безопасности, и, соответственно, провели обсуждение существующих и потенциальных угроз в сфере ИКТ в этом конкретном контексте. Напомнив об угрозах, о выявлении которых говорилось в первом ежегодном докладе о проделанной работе, докладе РГОС 2021 года и докладах ГПЭ, государства вновь выразили растущую обеспокоенность тем, что в нынешней сложной геополитической обстановке угрозы, связанные с использованием ИКТ в контексте международной безопасности, усилились и существенным образом изменились.

11. Государства напомнили, что ряд государств занимается наращиванием потенциала в сфере ИКТ для военных целей[8]. Они напомнили также, что применение ИКТ в будущих конфликтах между государствами становится все более вероятным, и отметили, что ИКТ уже используются в конфликтах в различных регионах. 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[9].

12. Кроме того, государства выразили особую озабоченность ростом злонамеренной деятельности в сфере ИКТ, затрагивающей объекты критически важной инфраструктуры и объекты критически важной информационной инфраструктуры, включая объекты, обеспечивающие предоставление самых необходимых трансграничных или международных услуг, что может привести к цепной реакции на национальном, региональном и глобальном уровнях, а также злонамеренной деятельности в сфере ИКТ, направленной против гуманитарных организаций. Особо отмечалось влияние угроз в сфере ИКТ на различные отрасли, включая здравоохранение, морское судоходство, авиацию и энергетику.

---

[8] Доклад РГОС 2021 года (A/75/816), приложение I, пункт 16.

[9] Доклад РГОС 2021 года (A/75/816), приложение I, пункт 16.

13. Государства также особо отметили, что злонамеренные действия с использованием ИКТ, направленные против объектов критически важной 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, вызывают реальную и растущую озабоченность[10]. Особую озабоченность государства выразили по поводу злонамеренной деятельности в сфере ИКТ, направленной на вмешательство во внутренние дела государств.

14. Более того, государства с тревогой отметили рост злонамеренного использования государствами скрытых информационных кампаний с применением ИКТ для влияния на процессы, системы и общую стабильность других государств. Такие действия подрывают доверие, могут потенциально привести к эскалации ситуации и угрожать международному миру и безопасности. Они также могут наносить прямой и косвенный вред людям[11].

15. Государства также выразили озабоченность по поводу злоупотребления факторами уязвимости информационно-коммуникационных продуктов и использования скрытых вредоносных функций, особенно в тех случаях, когда это влияет на международный мир и безопасность. Кроме того, государства отметили значительную угрозу целостности цепочек поставок. Государства также особо отметили опасность, которую представляют вредоносные программы, такие как вирусы-вымогатели, а также вайперы (стиратели) и троянские программы, и такие методы, как фишинг и распределенные атаки типа «отказ в обслуживании» (DDoS).

16. Далее, государства выразили обеспокоенность безответственным и потенциально злонамеренным использованием имеющихся возможностей ИКТ, в том числе государствами. Государства также выразили обеспокоенность по поводу использования средств ИКТ злоумышленниками.

17. Государства отметили, что новые и новейшие технологии расширяют возможности для развития. Однако их постоянно изменяющиеся свойства и характеристики также расширяют диапазон для совершения атак, создавая новые векторы и уязвимые места, которыми можно воспользоваться для вредоносной деятельности с применением ИКТ[12], что потенциально может повлиять на использование ИКТ в контексте международной безопасности. Государства также отметили возрастающую актуальность защиты данных и обеспечения их безопасности, учитывая увеличение объема и агрегирование данных, связанных с новыми и развивающимися технологиями. Государства с озабоченностью отметили, что обеспечение защиты от злонамеренного использования уязвимостей в операционных технологиях и взаимосвязанных вычислительных устройствах, платформах, машинах или объектах, составляющих Интернет вещей, становится серьезным вызовом.

18. Государства также обратили внимание на необходимость учета гендерных аспектов при борьбе с угрозами в сфере ИКТ и на конкретные риски, с которыми сталкиваются люди, находящиеся в уязвимом положении. Государства вновь подчеркнули, что преимуществами цифровых технологий пользуются не все в равной степени, и, соответственно, отметили необходимость уделить должное

---

[10] Доклад РГОС 2021 года (A/75/816), приложение I, пункт 18.

[11] Доклад ГПЭ 2021 года (A/76/135), пункт 9; и принятая на основе консенсуса резолюция 76/19 Генеральной Ассамблеи.

[12] Первый ежегодный доклад РГОС о проделанной работе (A/77/275), пункт 11; доклад ГПЭ 2021 года (A/76/135), пункт 11; и принятая на основе консенсуса резолюция 76/19 Генеральной Ассамблеи.

внимание растущему цифровому разрыву в контексте ускорения реализации целей в области устойчивого развития, учитывая при этом национальные потребности и приоритеты государств.

19. Государства напомнили, что любое использование ИКТ государствами таким образом, который противоречит их обязательствам в соответствие с рамками ответственного поведения государств в области использования ИКТ, включающими добровольные нормы, международное право и меры укрепления доверия, подрывает международный мир и безопасность, доверие и стабильность в отношениях между государствами[13].

20. Государства выразили обеспокоенность тем, что недостаточная информированность о существующих и потенциальных угрозах и отсутствие надлежащих возможностей для выявления злонамеренных действий с использованием ИКТ, а также соответствующей защиты и реагирования могут сделать их более уязвимыми[14]. Учитывая меняющуюся обстановку в плане угроз, связанных с использованием ИКТ в контексте международной безопасности, и принимая во внимание, что от этих угроз не защищено ни одно государство, государства особо подчеркнули, что необходимо в срочном порядке повышать информированность и углублять понимание таких угроз, а также продолжать разработку и осуществление совместных мер[15] и инициатив по наращиванию потенциала в соответствии с кумулятивными и эволюционирующими рамками ответственного поведения государств.

**Рекомендуемые дальнейшие действия**

21. **Государства продолжат в рамках РГОС обмен мнениями о существующих и потенциальных угрозах безопасности в сфере использования ИКТ, которые способны повлиять на международный мир и безопасность, и обсуждение возможных совместных мер по устранению этих угроз, признавая в этой связи, что приверженность всех государств соблюдению и применению рамок ответственного поведения государств в области использования ИКТ и подтверждение ими таких намерений все также имеют основополагающее значение для устранения существующих и потенциальных угроз международной безопасности, связанных с ИКТ.**

22. **Кроме того, РГОС следует созвать специальное межсессионное совещание по существующим и потенциальным угрозам безопасности в сфере использования ИКТ с участием соответствующих экспертов, приглашенных председателем РГОС при должном учете справедливой географической представленности.**

## C. Правила, нормы и принципы ответственного поведения государств

23. В ходе четвертой, пятой, а также неофициальных сессий РГОС государства продолжили обсуждение правил, норм и принципов ответственного поведения государств. Подтвердив значение кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ, государства выступили с конкретными, ориентированными на практические действия предложениями в отношении правил, норм и принципов. Ниже приводится

[13] Первый ежегодный доклад РГОС о проделанной работе (A/77/275), пункт 12; и доклад РГОС 2021 года (A/75/816), приложение I, пункт 17.

[14] Доклад РГОС 2021 года (A/75/816), приложение I, пункт 20.

[15] Доклад РГОС 2021 года (A/75/816), приложение I, пункт 22.

неисчерпывающий перечень предложений, которые были в разной степени поддержаны государствами и которые могут быть доработаны и дополнены на предстоящих сессиях РГОС:

a) государства сослались на мандат РГОС, который содержится в резолюции 75/240, и, в частности, предусматривает: «дальнейшую выработку норм, правил и принципов ответственного поведения государств и путей их имплементации, при необходимости, внесения в них изменений или формулирования дополнительных правил поведения»[16];

b) 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[17];

c) государства подчеркнули важность защиты критически важной инфраструктуры (КВИ) и критически важной информационной инфраструктуры (КВИИ). Государства особо отметили, что деятельность с использованием ИКТ, которая наносит преднамеренный ущерб КВИ и КВИИ или иным образом препятствует использованию и функционированию КВИ и КВИИ, используемых для обслуживания населения, может вызвать цепную реакцию и иметь внутренние, региональные и глобальные последствия. Она создает повышенный риск причинения вреда населению, а также может носить эскалационный характер[18]. Таким образом, государства подчеркнули необходимость дальнейшего усиления мер по защите всех объектов КВИ и КВИИ от угроз в сфере ИКТ и предложили активизировать обмен передовым опытом в области защиты КВИ и КВИИ, включая обмен информацией о национальной политике, и восстановления после инцидентов в сфере использования ИКТ, затрагивающих КВИ и КВИИ. В этой связи государства сослались на резолюцию 58/199 Генеральной Ассамблеи «Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур»[19] и на приложение к ней. Кроме того, государства предложили оказывать поддержку развивающимся странам и малым государствам по их просьбе в выявлении ими национальных объектов КВИ и КВИИ;

d) государства по-прежнему подчеркивали, что можно активизировать сотрудничество и оказание помощи для обеспечения целостности каналов поставок и предотвращения использования скрытых вредоносных функций. Разумные меры для поощрения открытости и обеспечения целостности, стабильности и безопасности каналов поставок могут включать разработку стратегий и программ, направленных на объективное содействие внедрению поставщиками и продавцами оборудования и систем ИКТ передовых методов в целях укрепления международного доверия к целостности и безопасности ИКТ-продуктов и услуг, повышения качества и содействия наличию выбора, принятие совместных мер, таких как обмен передовым опытом по управлению рисками в отношении каналов поставок; разработку и внедрение совместимых на глобальном уровне общих правил и стандартов обеспечения безопасности каналов поставок; и

---

[16] Резолюция 75/240 Генеральной Ассамблеи, пункт 1 постановляющей части.

[17] Доклад РГОС 2021 года (A/75/816), приложение I, пункты 64 и 65.

[18] Доклад ГПЭ 2021 года (A/76/135), пункт 42; и принятая на основе консенсуса резолюция 76/19 Генеральной Ассамблеи.

[19] Доклад ГПЭ 2021 года (A/76/135), пункт 48; и принятая на основе консенсуса резолюция 76/19 Генеральной Ассамблеи.

применение других подходов, направленных на снижение уровня уязвимости каналов поставок;

e) государства отметили важнейшую роль, которую играет частный сектор в обеспечении открытости и целостности, стабильности и безопасности каналов поставок, а также предупреждении распространения злонамеренных программных и технических средств в сфере ИКТ и использования скрытых вредоносных функций. Было предложено, чтобы в дополнение к описанным выше шагам и мерам государства продолжали укреплять партнерство с частным сектором для совместного повышения безопасности в сфере использования ИКТ и самих ИКТ. Кроме того, государствам следует и далее содействовать тому, чтобы частный сектор играл надлежащую роль в укреплении безопасности в сфере использования ИКТ и самих ИКТ, включая безопасность каналов поставок ИКТ-продуктов, в соответствии с национальными законами и правилами стран, в которых они работают;

f) государства подчеркнули необходимость дальнейшего содействия государствам в реализации правил, норм и принципов ответственного поведения государств при использовании ИКТ. Государствам предлагается рассмотреть возможность:

i) проведения, на добровольной основе, обзора практики имплементации ими на национальном уровне правил, норм и принципов ответственного поведения государств, а также соответствующих потребностей в наращивании потенциала. Государства могут обмениваться информацией о таких исследованиях в рамках доклада Генерального секретаря о достижениях в сфере ИКТ в контексте международной безопасности, а также Обзора хода реализации на национальном уровне, в соответствии с рекомендациями, содержащимися в докладе РГОС 2021 года[20];

ii) участия, на добровольной основе, в разработке и использовании дополнительного руководства или контрольного перечня по имплементации норм, дорабатывая и используя в качестве основы выводы и рекомендации, согласованные в предыдущих докладах РГОС и ГПЭ;

g) государства особо подчеркнули необходимость дальнейших целенаправленных обсуждений правил, норм и принципов ответственного поведения государств при использовании ИКТ;

h) что касается рассмотрения предложений по данному вопросу, то государства предложили продолжить обсуждение неисчерпывающего перечня предложений относительно разработки правил, норм и принципов ответственного поведения государств (доклад РГОС 2021 года, приложение к резюме Председателя)[21] в соответствии с рекомендацией, содержащейся в докладе РГОС 2021 года[22].

---

[20] Доклад РГОС 2021 года (A/75/816), приложение I, пункты 64 и 65.
[21] Доклад РГОС 2021 года (A/75/816), приложение II.
[22] Доклад РГОС 2021 года (A/75/816), приложение I, пункт 33.

**Рекомендуемые дальнейшие действия**

24. **Государства продолжат в рамках РГОС обмен мнениями о правилах, нормах и принципах ответственного поведения государств при использовании ИКТ с учетом подпунктов 23 a)–h) выше на шестой, седьмой и восьмой сессиях РГОС.**

25. **Кроме того, на шестой, седьмой и восьмой сессиях РГОС государствам предлагается провести целенаправленные обсуждения по следующим вопросам: a) усиление мер по защите КВИ и КВИИ от угроз в сфере ИКТ, включая обмен передовым опытом по обнаружению, защите от инцидентов в сфере использования ИКТ, реагированию на них и восстановлению после них, а также оказание поддержки развивающимся странам и малым государствам по их просьбе в выявлении национальных объектов КВИ и КВИИ; и b) дальнейшее сотрудничество и оказание помощи для обеспечения целостности каналов поставок и предотвращения использования скрытых вредоносных функций.**

26. **Государствам предлагается разработать дополнительное руководство, включая контрольный перечень, по имплементации норм с учетом ранее достигнутых договоренностей. Председателю РГОС предлагается подготовить первоначальный проект такого контрольного перечня для рассмотрения государствами.**

27. **Председателю РГОС предлагается созвать специальное межсессионное совещание для дальнейшего обсуждения правил, норм и принципов ответственного поведения государств при использовании ИКТ с учетом подпунктов 23 a)–h) выше. В этой связи председатель РГОС мог бы пригласить для проведения брифингов в рамках этих обсуждений соответствующих экспертов из региональных и субрегиональных организаций, деловых кругов, неправительственных организаций и научно-академического сообщества, обеспечив при этом должный учет справедливой географической представленности.**

## D. Международное право

28. В ходе четвертой и пятой, а также неофициальных сессий РГОС государства, подтвердив значение кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ, а также подтвердив, что международное право, в частности Устав Организации Объединенных Наций, применимо и необходимо для поддержания мира, безопасности и стабильности и содействия созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды, продолжили обсуждение того, как международное право применяется к использованию ИКТ. РГОС провела целенаправленное углубленное обсуждение тем из неисчерпывающего перечня, приведенного в подпунктах 15 a) и b) первого ежегодного доклада о проделанной работе, а также, в соответствующих случаях, предложений, содержащихся в докладе РГОС 2021 года и резюме Председателя[23].

[23] Первый ежегодный доклад РГОС о проделанной работе (A/77/275), раздел «Международное право», подраздел «Рекомендуемые дальнейшие действия», пункт 2.

29. При проведении этих целенаправленных обсуждений государства руководствовались содержащейся в первом ежегодном докладе о проделанной работе рекомендацией о проведении целенаправленных обсуждений тем из неисчерпывающего перечня, приведенного в следующих пунктах[24]:

a) «РГОС могла бы проводить обсуждение конкретных тем, касающихся международного права. В ходе таких обсуждений следует сосредоточиться на определении сфер близости позиций и консенсуса. Неисчерпывающий открытый список тем, предложенных государствами для дальнейшего обсуждения и касающихся международного права, включает следующие темы: как международное право, в частности Устав Организации Объединенных Наций, применяется к использованию ИКТ; суверенитет; суверенное равенство; невмешательство во внутренние дела других государств; мирное урегулирование споров; ответственность государств и должная осмотрительность; уважение прав человека и основных свобод; вопрос о существовании пробелов в общем понимании того, как применяется международное право; и предложения, содержащиеся в докладе РГОС 2021 года и резюме Председателя, если они релевантны»;

b) РГОС отметила в связи с рекомендациями, содержащимися в докладе РГОС 2021 года и докладе ГПЭ 2021 года, следующее:

i) «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»[25];

ii) «группа отмечает, что нормы международного гуманитарного права применимы только в ситуациях вооруженных конфликтов. Она напоминает об установленных международно-правовых принципах, включая, где это применимо, принципы гуманности, необходимости, соразмерности и избирательности, которые были отмечены в докладе 2015 года. Группа признает необходимость дальнейшего изучения вопроса о том, как и когда эти принципы применяются к использованию ИКТ государствами, и подчеркивает, что напоминание об этих принципах ни в коем случае не узаконивает и не поощряет конфликты»[26];

---

[24] Первый ежегодный доклад РГОС о проделанной работе (A/77/275), пункт 15 b) i) и ii) и раздел «Международное право», подраздел «Рекомендуемые дальнейшие действия», пункт 2.

[25] Доклад РГОС 2021 года (A/75/816), приложение I, пункт 80.

[26] Доклад ГПЭ 2021 года (A/76/135), пункт 71 f); принятая на основе консенсуса резолюция 76/19 Генеральной Ассамблеи.

30. В ходе целенаправленных обсуждений РГОС вопросов применения международного права к использованию ИКТ государства в частности:

a) подтвердили принципы государственного суверенитета и суверенного равенства;

b) сослались на пункт 3 статьи 2 Устава Организации Объединенных Наций, который гласит, что «все члены разрешают свои международные споры мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость»[27]; и пункт 1 статьи 33 Устава Организации Объединенных Наций, который гласит, что «стороны, участвующие в любом споре, продолжение которого могло бы угрожать поддержанию международного мира и безопасности, должны прежде всего стараться разрешить спор путем переговоров, обследования, посредничества, примирения, арбитража, судебного разбирательства, обращения к региональным органам или соглашениям или иными мирными средствами по своему выбору»[28];

c) сослались также на пункт 4 статьи 2 Устава Организации Объединенных Наций, который гласит, что «все члены Организации Объединенных Наций воздерживаются в их международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями Объединенных Наций»;

d) подтвердили, что, в соответствии с принципом невмешательства, государства не должны прямо или косвенно вмешиваться во внутренние дела другого государства, в том числе с помощью ИКТ[29];

31. Государства также внесли дополнительные конкретные, ориентированные на практические действия предложения в отношении международного права, а именно:

a) государства отметили, что межсессионные обсуждения углубили и обогатили продолжающиеся обсуждения вопросов применения международного права к использованию ИКТ, и предложили провести дополнительные заседания в следующий межсессионный период работы РГОС;

b) государства отметили также, что обмен национальными мнениями может способствовать формированию общего понимания того, как международное право применяется к использованию ИКТ, и призвали продолжать добровольный обмен национальными мнениями по международному праву, который может включать национальные заявления и практику государств в отношении того, как международное право применяется к использованию ИКТ государствами. Кроме того, в выработке такого общего понимания государствам могут помочь соответствующие исследования и мнения экспертов в области международного права;

c) признавая существующие инициативы по наращиванию потенциала в области международного права, государства далее подчеркнули настоятельную необходимость продолжения такой работы по наращиванию потенциала, в том числе с целью обеспечения возможностей для всех государств на равных участвовать в выработке общего понимания того, как международное право применяется к использованию ИКТ. Такая работа по наращиванию потенциала может

---

[27] Пункт 3 статьи 2 Устава Организации Объединенных Наций.

[28] Пункт 1 статьи 33 Устава Организации Объединенных Наций.

[29] Доклад ГПЭ 2021 года (A/76/135), пункт 71 c); и принятая на основе консенсуса резолюция 76/19 Генеральной Ассамблеи.

включать проведение семинаров, учебных курсов, обмен передовым опытом на международном, межрегиональном, региональном и субрегиональном уровнях, а также, при необходимости, использование опыта соответствующих региональных организаций и должна осуществляться в соответствии с принципами наращивания потенциала, изложенными в пункте 56 доклада РГОС 2021 года.

32. Отмечая возможность разработки в будущем, при необходимости, дополнительных имеющих обязательную силу обязательств, государства обсудили необходимость рассмотрения вопроса о том, существуют ли какие-либо пробелы в вопросах применения действующего международного права к использованию ИКТ, и дальнейшего рассмотрения вопроса о разработке дополнительных юридически обязывающих обязательств[30].

**Рекомендуемые дальнейшие действия**

33. **Государства продолжат участвовать в проводимых в рамках РГОС целенаправленных обсуждениях вопросов применения международного права к использованию ИКТ, опираясь, в соответствующих случаях, на темы из неисчерпывающего перечня, приведенного в подпунктах 29 a) и b) выше, а также на предложения по теме международного права, содержащиеся в докладе РГОС 2021 года и резюме Председателя.**

34. **В развитие обсуждений, состоявшихся на четвертой и пятой сессиях РГОС, государствам предлагается продолжать добровольный обмен национальными мнениями, в которые могут входить национальные заявления и практика государств, о том, как международное право применяется к использованию ИКТ. Секретариату Организации Объединенных Наций предлагается разместить информацию об этих мнениях на веб-сайте РГОС для ознакомления всех государств и для дальнейшего обсуждения РГОС на ее шестой, седьмой и восьмой сессиях.**

35. **Председателю РГОС также предлагается созвать специальное межсессионное совещание по вопросам применения международного права к использованию ИКТ. В этой связи председатель РГОС мог бы, обеспечив при этом должный учет справедливой географической представленности и национального контекста, организовать дополнительные брифинги экспертов по вопросам применения международного права к использованию ИКТ.**

36. **Государствам, которые имеют такую возможность, следует продолжать, руководствуясь соображениями непредвзятости и объективности, поддерживать дополнительные усилия, в том числе в рамках деятельности Организации Объединенных Наций, по наращиванию потенциала в области международного права, с тем чтобы все государства могли способствовать достижению общего понимания того, как международное право применяется к использованию ИКТ и содействовать достижению консенсуса в международном сообществе. Такие усилия по наращиванию потенциала должны предприниматься в соответствии с принципами наращивания потенциала, изложенными в пункте 56 доклада РГОС 2021 года.**

[30] В связи с этим было внесено предложение, отраженное в приложении D.

## E. Меры укрепления доверия

37. В ходе четвертой, пятой, а также неофициальных сессий РГОС государства продолжили обсуждение мер укрепления доверия (МД). Подтвердив значение кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ, государства выступили с конкретными, ориентированными на практические действия предложениями в отношении мер укрепления доверия. Ниже приводится неисчерпывающий перечень предложений, которые были в разной степени поддержаны государствами и которые могут быть доработаны и дополнены на предстоящих сессиях РГОС:

a) ссылаясь на то, что в первом ежегодном докладе о проделанной работе государства договорились составить, опираясь на результаты проделанной на региональном уровне работы, глобальный межправительственный реестр контактных пунктов[31], государства предложили РГОС принять документ под названием «Элементы разработки и введения в действие глобального межправительственного реестра контактных пунктов», содержащийся в приложении A к настоящему докладу, в качестве дальнейших мер по введению в действие глобального реестра контактных пунктов;

b) государства признали, что формирование и введение в действие глобального реестра контактных пунктов является важным шагом на пути укрепления доверия между государствами на глобальном уровне. Государства также признали, что глобальный реестр контактных пунктов может способствовать имплементации других мер укрепления доверия на глобальном уровне, которые могут содействовать созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. В этой связи государства, ссылаясь на рекомендации по мерам укрепления доверия, содержащиеся в консенсусных докладах, предложили составить на их основе первоначальный перечень добровольных глобальных мер укрепления доверия для реализации государствами, в том числе с помощью глобального реестра контактных пунктов;

c) в дополнение к уже согласованным мерам укрепления доверия, содержащимся в предыдущих докладах Организации Объединенных Наций, государства также предложили дополнительные меры, которые со временем могут быть признаны в качестве дополнительных мер укрепления доверия на глобальном уровне. Они включают следующие элементы мер укрепления доверия, основанные на глобальном реестре контактных пунктов (при этом следует отметить, что все эти предложения также включены в качестве оперативных элементов в документ, содержащийся в приложении A к настоящему докладу):

i) проверка связи в виде «пинг-тестов»;

ii) добровольный обмен информацией, в том числе при возникновении требующего безотлагательного внимания или значительного инцидента в сфере использования ИКТ, осуществляемый через глобальный реестр контактных пунктов;

iii) тренировочные занятия для моделирования практических аспектов участия в глобальном реестре контактных пунктов;

---

[31] Первый ежегодный доклад РГОС о проделанной работе (A/77/275), раздел «Меры укрепления доверия», подраздел «Рекомендуемые дальнейшие действия», пункт 2.

iv) регулярные очные или виртуальные встречи контактных пунктов для обмена практической информацией и опытом по введению в действие и использованию глобального реестра контактных пунктов на добровольной основе;

d) государства особо отметили важность обеспечения быстрого устранения уязвимостей ИКТ в целях снижения вероятности их использования злоумышленниками. Своевременное обнаружение и ответственное и объективное раскрытие информации об уязвимостях ИКТ, сопровождающиеся соответствующей отчетностью, могут предотвратить вредные или угрожающие действия, укрепить доверие и уверенность, а также уменьшить число связанных с этим угроз международной безопасности и стабильности[32]. Было предложено продолжить обсуждение этого вопроса в рамках РГОС;

e) государства отметили, что обмен национальными мнениями относительно технических терминов и терминологии в сфере ИКТ может способствовать повышению транспарентности и взаимопонимания между государствами;

f) было высказано предложение о том, что аспекты мер укрепления доверия могут, сообразно обстоятельствам, и далее включать взаимодействие с региональными и субрегиональными организациями и заинтересованными сторонами, включая представителей деловых кругов, неправительственных организаций и научно-академического сообщества;

g) государства вновь подчеркнули, что сама РГОС служит одной из мер укрепления доверия, являясь форумом для обсуждения вопросов, по которым имеется согласие, и вопросов, по которым согласие пока не достигнуто.

**Рекомендуемые дальнейшие действия**

38. **Государства продолжат в рамках РГОС обмен мнениями о разработке и имплементации мер укрепления доверия, в том числе о возможной разработке дополнительных мер укрепления доверия.**

39. **Ссылаясь на то, что в первом ежегодном докладе РГОС о проделанной работе государства договорились о создании глобального межправительственного реестра контактных пунктов[33], государства далее соглашаются принять документ под названием «Элементы разработки и введения в действие глобального межправительственного реестра контактных пунктов», содержащийся в приложении A к настоящему докладу, в рамках дальнейших мер по введению в действие глобального реестра контактных пунктов.**

40. **Государствам предлагается продолжить обсуждение и участие во введении в действие и использовании глобального реестра контактных пунктов на шестой, седьмой и восьмой сессиях РГОС, в том числе в контексте подпунктов 37 b) и c) настоящего доклада.**

41. **Государства рекомендуют первоначальный, неисчерпывающий перечень добровольных глобальных мер укрепления доверия, содержащийся в приложении B, составленный на основе мер укрепления доверия, согласованных консенсусом в докладе РГОС 2021 года, а также в первом и втором ежегодных докладах нынешней РГОС о проделанной работе. Председателю РГОС предлагается содействовать продолжению обсуждения путей**

---

[32] Доклад ГПЭ 2021 года (A/76/135), пункт 60; и принятая на основе консенсуса резолюция 76/19 Генеральной Ассамблеи.

[33] Первый ежегодный доклад РГОС о проделанной работе (A/77/275), раздел «Меры укрепления доверия», подраздел «Рекомендуемые дальнейшие действия», пункт 2.

**разработки, дополнения и введения в действие этих мер укрепления доверия, в том числе, среди прочего, путем: a) наращивания соответствующего потенциала; и b) внедрения глобального реестра контактных пунктов.**

42. **Государствам предлагается на добровольной основе обмениваться национальными мнениями относительно технических терминов и терминологии в сфере ИКТ для повышения транспарентности и взаимопонимания между государствами.**

## F. Наращивание потенциала

43. В ходе четвертой, пятой, а также неофициальных сессий РГОС государства продолжили обсуждение вопросов наращивания потенциала ИКТ в контексте международной безопасности. Подтвердив значение кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ, государства выступили с конкретными, ориентированными на практические действия предложениями в отношении усилий по наращиванию потенциала. Ниже приводится неисчерпывающий перечень предложений, которые были в разной степени поддержаны государствами и которые могут быть доработаны и дополнены на предстоящих сессиях РГОС:

a) государства предложили более полно учитывать принципы наращивания потенциала, принятые в докладе РГОС 2021 года, в инициативах по наращиванию потенциала в области безопасности при использовании ИКТ[34]. Кроме того, государства продолжали поощрять усилия по содействию наращиванию потенциала с учетом гендерных аспектов, в том числе путем интеграции гендерных аспектов в национальную политику в области ИКТ и наращивания потенциала, а также разработки контрольных перечней или вопросников для выявления потребностей и пробелов в этой области;

b) государства подчеркнули ценность сотрудничества Юг — Юг, трехстороннего, субрегионального и регионального сотрудничества, в дополнение к сотрудничеству Север — Юг;

c) РГОС могла бы способствовать более глубокому пониманию потребностей развивающихся стран в целях сокращения цифрового разрыва посредством целенаправленных усилий по наращиванию потенциала, работая над обеспечением наличия у всех государств потенциала, необходимого для соблюдения и применения кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ;

d) государства подчеркнули, что необходима дальнейшая координация усилий по наращиванию потенциала в области безопасности ИКТ, и Организация Объединенных Наций могла бы сыграть важную роль в этом отношении, в том числе путем анализа потребностей и выявления пробелов в наращивании потенциала государств с помощью инструментов и обследований, а также облегчения доступа государств к программам наращивания потенциала. Секретариату Организации Объединенных Наций было предложено собрать воедино существующие программы и инициативы по наращиванию потенциала, связанные с вопросами безопасности при использовании ИКТ в рамках Организации Объединенных Наций и за ее пределами, на глобальном и региональном уровнях, чтобы способствовать дальнейшему обсуждению в рамках РГОС путей

[34] Доклад РГОС 2021 года (A/75/816), приложение I, пункт 56.

повышения синергетического эффекта, координации и расширения доступа к предлагаемым программам по наращиванию потенциала;

e) отмечая существующее финансирование усилий по наращиванию потенциала в области безопасности при использовании ИКТ, государства могут в то же время продолжить рассмотрение дополнительных возможностей финансирования, ориентированные именно на наращивание потенциала в вопросах безопасности при использовании ИКТ, в том числе путем возможной координации и интеграции с существующими программами и фондами развития;

f) государства обсудили инициативу по созданию глобального портала сотрудничества в области кибербезопасности и предложили сделать его практичным и нейтральным, созданным по инициативе государств-участников модульным инструментом «единого окна» для государств, разработанным под эгидой Организации Объединенных Наций. Также высказывались предложения об обеспечении, при необходимости, повышения эффективности этого портала за счет его взаимодействия с другими существующими порталами. Кроме того, государства предложили включить в инициативу по созданию такого глобального портала создание хранилища примеров передового опыта по наращиванию потенциала в области безопасности ИКТ. В связи с этим государства также подчеркнули важность углубления знаний и понимания ранее достигнутых договоренностей, содержащихся в докладах РГОС и ГПЭ, для использования их в текущей работе;

g) государства признали, что сама РГОС могла бы стать платформой для продолжения обмена мнениями и идеями относительно усилий по наращиванию потенциала в вопросах безопасности при использовании ИКТ, в том числе относительно того, как лучше использовать существующие инициативы, чтобы поддержать государства в развитии институциональных возможностей применения рамок ответственного поведения государства при использовании ИКТ. Было предложено обсудить возможности, которые могут помочь государствам в этом вопросе. На основе результативного круглого стола по наращиванию потенциала, созванного председателем РГОС в мае 2023 года, было предложено также проводить дальнейшие круглые столы по наращиванию потенциала под эгидой РГОС с участием соответствующих заинтересованных сторон и специалистов-практиков для обмена передовым опытом в области наращивания потенциала в вопросах международной безопасности при использовании ИКТ;

h) государства выразили обеспокоенность тем, что недостаточная информированность о существующих и потенциальных угрозах и отсутствие надлежащих возможностей для выявления злонамеренных действий с использованием ИКТ, а также соответствующей защиты и реагирования могут сделать их более уязвимыми[35]. В этой связи государства обсудили предложение о поощрении дальнейшего технического обмена информацией об угрозах в сфере ИКТ с целью расширения потенциала государств в деле выявления и обнаружения злонамеренной деятельности в сфере ИКТ, защиты от нее и содействия информированному реагированию на нее, принимая во внимание и дополняя существующие механизмы, такие как каналы взаимодействия групп реагирования на компьютерные инциденты друг с другом;

i) государства, в том числе через РГОС, могут продолжать укреплять координацию и сотрудничество между государствами и заинтересованными сторонами, включая представителей деловых кругов, неправительственных организаций и научно-академического сообщества. Государства отметили, что заинтересованные стороны уже играют важную роль в рамках налаженных с

[35] Доклад РГОС 2021 года (A/75/816), приложение I, пункт 20.

государствами партнерских отношений, в том числе в образовательных и исследовательских целях. Государства также признали необходимость наращивания потенциала в области выявления заинтересованных сторон и налаживания с ними конструктивного взаимодействия с целью укрепления процесса выработки политики и установления доверия для сотрудничества с заинтересованными сторонами в борьбе с инцидентами, связанными с безопасностью в сфере использования ИКТ.

**Рекомендуемые дальнейшие действия**

44. **Государства продолжат в рамках РГОС обмен мнениями о наращивании потенциала в связи с вопросами безопасности при использовании ИКТ, в том числе по подпунктам 43 a)–i) выше. Государствам также предлагается продолжить целенаправленные обсуждения вопросов более всестороннего учета в инициативах по наращиванию потенциала в области безопасности при использовании ИКТ принципов наращивания потенциала, принятых в докладе РГОС 2021 года (см. приложение C).**

45. **Председателю РГОС предлагается наладить взаимодействие с соответствующими подразделениями Организации Объединенных Наций и международными организациями, предлагающими программы наращивания потенциала в области безопасности при использовании ИКТ, и призвать их, руководствуясь необходимостью и целесообразностью и действуя в соответствии с их мандатами, согласовать свои программы наращивания потенциала для обеспечения дальнейшей поддержки государств в имплементации ими рамок ответственного поведения государств в области использования ИКТ и их работы по созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.**

46. **Секретариату Организации Объединенных Наций предлагается провести картирование процесса в консультации с соответствующими структурами с целью изучения ситуации с программами и инициативами по наращиванию потенциала в рамках Организации Объединенных Наций и за ее пределами, на глобальном и региональном уровнях, в том числе путем выяснения мнений государств-членов. Секретариату Организации Объединенных Наций также предлагается подготовить доклад с результатами такого картирования и представить его на седьмой сессии РГОС, тем самым поддержав работу государств по оценке существующих усилий по наращиванию потенциала в области безопасности ИКТ и способствовать дальнейшему взаимоусилению и координации таких усилий.**

47. **Государствам предлагается продолжить обсуждение предложения о создании под эгидой Организации Объединенных Наций глобального портала сотрудничества в области кибербезопасности как инструмента «одного окна» для государств. Возможно продолжение обсуждений способов повышения эффективности этого портала за счет его взаимодействия с другими существующими порталами**

48. **Председателю РГОС предлагается созвать в межсессионный период специальное заседание в формате глобального круглого стола по наращиванию потенциала по обеспечению безопасности в сфере ИКТ в целях обеспечения возможности обмена информацией и передовым опытом. В заседании круглого стола могут принять участие специалисты-практики в области наращивания потенциала, а также представители заинтересованных государств и заинтересованных сторон, включая представителей деловых кругов, неправительственных организаций и научно-академического**

**сообщества, при должном учете справедливой географической представленности.**

49. **В целях углубления знаний и понимания ранее достигнутых договоренностей, содержащихся в докладах РГОС и ГПЭ, для использования их в текущей работе государств в рамках РГОС, государствам, которые имеют такую возможность, рекомендуется оказать Секретариату Организации Объединенных Наций поддержку в обновлении электронного учебного курса для дипломатов «Кибердипломатия» с целью выпуска обновленного курса в 2024 году. Секретариату Организации Объединенных Наций предлагается представить государствам обновленную информацию на шестой сессии РГОС. Секретариату Организации Объединенных Наций рекомендуется при обновлении курса консультироваться с соответствующими структурами.**

50. **Заинтересованным государствам рекомендуется разрабатывать и распространять добровольные контрольные перечни и другие инструменты, помогающие государствам учитывать принципы наращивания потенциала, изложенные в докладе РГОС 2021 года, в инициативах по наращиванию потенциала в вопросах безопасности при использовании ИКТ, а также разрабатывать и распространять инструменты, которые помогут государствам учитывать гендерные аспекты в таких усилиях по наращиванию потенциала.**

51. **Государствам, которые имеют такую возможность, предлагается продолжать поддерживать программы по наращиванию потенциала, в том числе в сотрудничестве, сообразно обстоятельствам, с региональными и субрегиональными организациями и другими заинтересованными сторонами, включая представителей деловых кругов, неправительственных организаций и научно-академического сообщества.**

## G. Регулярный институциональный диалог

52. В ходе четвертой и пятой сессий, а также неофициальных совещаний РГОС государства продолжили обсуждение вопросов регулярного институционального диалога. Подтвердив значение кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ, государства выступили с конкретными, ориентированными на практические действия предложениями в отношении институционального диалога. Данный неисчерпывающий перечень предложений, которые были в разной степени поддержаны государствами, может быть доработан и дополнен на предстоящих сессиях РГОС:

a) государства по-прежнему подчеркивали, что РГОС могла бы сыграть свою роль в повышении уровня информированности, укреплении доверия и углублении понимания в тех областях, в отношении которых общее понимание еще не достигнуто. Кроме того, работу РГОС следует поступательно выстраивать с опорой на ранее достигнутые договоренности. Государства признали центральную роль РГОС как действующего под эгидой Организации Объединенных Наций механизма поддержания диалога по вопросам безопасности при использовании ИКТ[36];

[36] Первый ежегодный доклад РГОС о проделанной работе (A/77/275), пункт 18 a).

b) в соответствии с рекомендацией, содержащейся в докладе РГОС 2021 года[37], и в первом ежегодном докладе РГОС о проделанной работе[38] государства углубили обсуждение предложения об учреждении программы действий по поощрению ответственного поведения государств при использовании ИКТ в контексте международной безопасности. Были высказаны и другие предложения, касающиеся регулярного институционального диалога, включая предложение о создании в будущем группы, комиссии, комитета или конференции под эгидой Организации Объединенных Наций.

53. С учетом широкого спектра предложенных возможных вариантов регулярного институционального диалога было предложено, чтобы в качестве первого шага по укреплению доверия и сближению позиций государства выдвинули предложения по определению общих элементов, которые могли бы лечь в основу разработки любого будущего механизма регулярного институционального диалога по вопросам безопасности в сфере использования ИКТ, а также было продолжено дальнейшее обсуждение предложений, определенных в подпунктах 52 a) и b).

**Рекомендуемые дальнейшие действия**

54. **Государства продолжат в рамках РГОС обмен мнениями о регулярном институциональном диалоге и предложениях государств о содействии регулярному институциональному диалогу по вопросам безопасности при использовании ИКТ с целью выработки общего понимания о наиболее эффективном формате будущего регулярного институционального диалога при широком участии государств под эгидой Организации Объединенных Наций.**

55. **Государства, договорившись продолжить обсуждение дополнительных элементов, в принципе согласны с тем, что будущий механизм регулярного институционального диалога будет основываться на следующих общих элементах:**

a) **это будет одновекторный, возглавляемый государствами постоянный механизм под эгидой Организации Объединенных Наций, подотчетный Первому комитету Генеральной Ассамблеи Организации Объединенных Наций;**

b) **целью будущего механизма будет дальнейшее содействие созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды;**

c) **в основу работы будущего механизма будут положены консенсусные договоренности о рамках ответственного поведения государств в области использования ИКТ, содержащиеся в предыдущих докладах РГОС и ГПЭ;**

d) **это будет открытый, инклюзивный, транспарентный, устойчивый и гибкий процесс, способный развиваться в соответствии с потребностями государств, а также с учетом изменений ИКТ-среды.**

56. **Государства признали важность принципа консенсуса как в отношении учреждения самого будущего механизма, так и в отношении процессов принятия решений в рамках этого механизма.**

---

[37] Доклад РГОС 2021 года (A/75/816), приложение I, пункт 77.

[38] Первый ежегодный доклад РГОС о проделанной работе (A/77/275), раздел «Регулярный институциональный диалог», подраздел «Рекомендуемые дальнейшие действия», пункт 2.

57. **Другие заинтересованные стороны, включая представителей деловых кругов, неправительственных организаций и научно-академического сообщества, могут вносить свой вклад в будущий регулярный институциональный диалог.**

58. **На шестой, седьмой и восьмой сессиях РГОС, а также на двух специализированных межсессионных совещаниях государствам предлагается продолжить участие в проводимых в рамках РГОС целенаправленных обсуждениях, касающихся дальнейшего рассмотрения предложений по поддержанию регулярного институционального диалога, включая программу действий. В ходе этих сессий государства будут также участвовать в целенаправленных обсуждениях, посвященных взаимосвязи программы действий и РГОС, а также сфере охвата, содержанию и структуре программы действий[39]. Секретариату Организации Объединенных Наций также предлагается проинформировать РГОС на ее шестой сессии о докладе Генерального секретаря, представленном Генеральной Ассамблее на ее семьдесят восьмой сессии[40].**

59. **Государствам, которые имеют такую возможность, следует продолжить рассмотрение вопроса о создании или поддержке спонсорских программ и других механизмов для обеспечения широкого участия в соответствующих процессах в рамках Организации Объединенных Наций.**

## H. Заключительные замечания

60. Государства отметили растущую активность и конструктивное участие делегаций из всех регионов в работе РГОС в течение последних пяти основных сессий. В ходе сессий государства внесли существенный вклад в работу РГОС. Государства и группы государств также представили РГОС рабочие документы с изложением своих национальных и групповых позиций, идей и инициатив по вопросам, входящим в мандат РГОС, перечень которых приведен в приложении D.

---

[39] Первый ежегодный доклад РГОС о проделанной работе (A/77/275), раздел «Регулярный институциональный диалог», подраздел «Рекомендуемые дальнейшие действия», пункт 2.

[40] A/78/76.

# Приложение A

## Элементы разработки и введения в действие глобального межправительственного реестра контактных пунктов

1. В соответствии с первым ежегодным докладом РГОС о проделанной работе, содержащимся в документе A/77/275, в котором государства согласились создать, опираясь на результаты проделанной на региональном уровне работы, глобальный межправительственный реестр контактных пунктов, в настоящем документе излагаются элементы, которые могут служить руководством для разработки и введения в действие такого реестра в сфере использования ИКТ в контексте международного мира и безопасности.

### Цели и принципы

2. Глобальный межправительственный реестр контактных пунктов сам по себе будет служить мерой укрепления доверия, а также обеспечит основу для имплементации других мер укрепления доверия, способных содействовать созданию открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды.

3. Предполагается, что реестр контактных пунктов будет носить добровольный, практический и нейтральный характер, разрабатываться и реализовываться в соответствии с принципами суверенитета, суверенного равенства, разрешения споров мирными средствами и невмешательства во внутренние дела других государств.

4. Реестр контактных пунктов будет учитывать и дополнять работу сетей групп реагирования на компьютерные инциденты и групп реагирования на инциденты в сфере кибербезопасности.

5. Основными целями создания реестра контактных пунктов являются:

a) усиление взаимодействия и сотрудничества между государствами, способствующее укреплению международного мира и безопасности, а также повышению транспарентности и предсказуемости;

b) содействие координации и связи между государствами, в том числе при возникновении требующего безотлагательного внимания или значительного инцидента в сфере использования ИКТ, для укрепления доверия между государствами, снижения напряженности и предотвращения недопонимания и неверного толкования, которые могут возникнуть в результате инцидентов в сфере использования ИКТ;

c) усиление коммуникации и обмена информацией и предоставление государствам, в том числе путем соответствующего наращивания потенциала, возможности содействовать предотвращению, обнаружению, реагированию и восстановлению, в частности, в отношении требующих безотлагательного внимания или значительных инцидентов в сфере использования ИКТ;

d) реестр контактных пунктов может способствовать обеспечению надежной и прямой связи между государствами в целях предотвращения и урегулирования серьезных инцидентов в сфере использования ИКТ и ослабления напряженности в кризисных ситуациях. Коммуникация между контактными пунктами может помочь снизить напряженность и предотвратить недопонимание и неверное толкование, которые могут возникнуть в результате инцидентов в сфере использования ИКТ, в том числе затрагивающих критически важную инфраструктуру и имеющих национальное, региональное или глобальное

значение. Они могут также расширить обмен информацией и помочь государствам более эффективно управлять инцидентом в сфере использования ИКТ и урегулировать его[1].

**Порядок работы**

6. **Доступ и участие.** Участие в реестре контактных пунктов, включая предоставление информации, будет осуществляться на добровольной основе. Государствам, желающим принять участие в реестре контактных пунктов, будет предоставлен доступ к реестру контактных пунктов.

7. **Требования к реестру.** Управление Организации Объединенных Наций по вопросам разоружения (УВРООН) будет выступать в качестве администратора реестра контактных пунктов, отвечая за разработку и введение в действие технических аспектов реестра контактных пунктов в соответствии со следующими требованиями:

a) информационная схема:

i) государства могут назначать в реестр, по возможности, как дипломатические, так и технические контактные пункты;

ii) государства могут назначить в качестве контактных пунктов либо уполномоченную национальную структуру/учреждение, либо конкретного представителя уполномоченной национальной структуры/учреждения;

iii) государства могут предоставить информацию о структуре/учреждении, контактную информацию (номер телефона и электронную почту), фамилию, имя и должность соответствующего контактного пункта (где это применимо), а также рабочие языки контактного пункта;

iv) каждая запись в реестр может представляться на любом официальном языке Организации Объединенных Наций; кроме того, приветствуется представление неофициального перевода на английский язык;

b) защита информации: реестр контактных пунктов будет размещен в Интернете на защищенном сайте. В реестре не будет размещаться конфиденциальная информация, которую передают или которой обмениваются контактные пункты. Связь между контактными пунктами, включая передачу конфиденциальной информации, будет осуществляться по взаимно согласованным каналам, в том числе, сообразно обстоятельствам, по защищенным каналам;

c) доступ к информации: государства могут запросить учетные данные для доступа к веб-сайту у УВРООН через свои постоянные представительства в Нью-Йорке. В целях общей информации на веб-сайте УВРООН будет размещена публичная веб-страница, содержащая общий обзор мандата реестра контактных пунктов;

d) управление информацией: по мере изменения представленной ими информации, содержащейся в реестре контактных пунктов, государства могут предоставлять соответствующие обновленные данные.

8. **Ведение реестра.** Администратору реестра предлагается раз в полгода проводить «пинг-тесты» для проверки актуальности информации в реестре. В рамках «пинг-теста» с контактными пунктами связывается администратор реестра и просит их в течение 48 часов ответить сообщением, свидетельствующим о получении запроса администратора реестра. В случае отсутствия ответа на

[1] Доклад ГПЭ 2021 года (A/76/135), пункт 76; и принятая на основе консенсуса резолюция 76/19 Генеральной Ассамблеи.

«пинг-тест» администратор реестра приложит все усилия, чтобы связаться с соответствующими органами власти данного государства и предложить им обновить информацию.

9. **Роли дипломатических и технических контактных пунктов.** Предусматривается, что дипломатические и технические контактные пункты будут выполнять разные функции. Соответственно, дипломатические контактные пункты будут общаться с другими дипломатическими контактными пунктами, а технические контактные пункты — с другими техническими контактными пунктами. Приветствуется координация между контактными пунктами из одного государства. При определении роли своих контактных пунктов в соответствии с национальной политикой и законодательством государства могут рассмотреть следующие предлагаемые функции:

a) дипломатический контактный пункт может устанавливать связь с другими дипломатическими контактными пунктами, в том числе при возникновении требующего безотлагательного внимания или значительного инцидента в сфере использования ИКТ, для предотвращения недопонимания и снижения напряженности. При необходимости дипломатические контактные пункты могут рассмотреть возможность доведения информации об инциденте до сведения должностных лиц более высокого уровня в рамках соответствующих национальных правительственных структур, чтобы в случае необходимости наладить дальнейшее взаимодействие между государствами. В соответствующих случаях дипломатический контактный пункт может представлять уполномоченное национальное ведомство, отвечающее за международное сотрудничество;

b) технический контактный пункт может связываться с другими техническими контактными пунктами, в том числе в случае требующего безотлагательного внимания или значительного инцидента в сфере использования ИКТ, с целью предоставления или запроса информации или помощи. Это может, в частности, принимать форму запроса информации, просьбы о конкретных действиях или о помощи. Технические контактные пункты могут также на добровольной основе обмениваться с другими техническими контактными пунктами передовым опытом, извлеченными уроками и другой соответствующей информацией о том, как облегчить предотвращение, обнаружение, реагирование и восстановление, в частности, в отношении требующих безотлагательного внимания или значительных инцидентов в сфере использования ИКТ. В соответствующих случаях техническим контактным пунктом может быть уполномоченное национальное ведомство, занимающееся вопросами безопасности ИКТ и отвечающее за предотвращение, обнаружение, реагирование и восстановление в отношении инцидентов в сфере использования ИКТ, например, национальные группы реагирования на компьютерные инциденты и группы реагирования на инциденты в сфере кибербезопасности.

10. **Взаимодействие между контактными пунктами.** Решение о том, как реагировать на сообщения, полученные через реестр контактных пунктов, и о содержании сообщений, передаваемых в ответ, принимается каждым государством самостоятельно. Любой обмен информацией осуществляется на добровольной основе и в соответствии с внутренними условиями, требованиями и законодательством соответствующих государств. Любое последующее сотрудничество и/или обмен информацией, а также выбор канала, по которому будет поддерживаться такая связь, будет осуществляться по взаимной договоренности. Первоначальное подтверждение получения сообщения не означает согласия с содержащейся в нем информацией и не наносит ущерба позиции государства-ответчика, равно как и не предопределяет любое последующее сообщение. Кроме того, уведомление государства о том, что его территория используется для

совершения противоправного деяния, само по себе также не подразумевает, что оно несет ответственность за это деяние[2]:

a) по желанию, контактные пункты могут использовать для взаимодействия с другими контактными пунктами типовые процедуры. В качестве первоначального шага, облегчающего общение, контактные пункты могут рассмотреть возможность использования на добровольной основе «Процедуры запроса» и «Процедуры ответа на запрос», содержащиеся в добавлении к настоящему приложению;

b) по желанию, контактные пункты могут также использовать для взаимодействия с другими контактными пунктами типовые шаблоны. В таких типовых шаблонах могут указываться виды требуемой информации при отправке сообщения, включая технические данные и характер запроса, но при этом эти шаблоны должны быть достаточно гибкими, чтобы обеспечить возможность коммуникации, даже при нехватке информации по некоторым вопросам[3]; государства продолжат работу по разработке таких типовых шаблонов в соответствии с поэтапным подходом к доработке реестра контактных пунктов.

11. **Обмен информацией.** Информация, которой обмениваются контактные пункты, должна оставаться конфиденциальной. Контактные пункты, участвующие в обмене информацией, должны передавать ее третьим сторонам только по взаимному согласию. Контактным пунктам рекомендуется вести учет всей информации, которой они обмениваются.

12. **Взаимодействие с другими реестрами.** Реестр контактных пунктов представляет собой глобальную межправительственную платформу, которая, если это необходимо и целесообразно, может быть дополнена за счет существующих усилий на региональном и субрегиональном уровнях. В этой связи государства отметили, что не все государства являются членами региональных и субрегиональных организаций и что не все такие организации ведут реестр контактных пунктов. Во избежание дублирования усилий государствам рекомендуется должным образом рассмотреть, сообразно обстоятельствам, вопрос о повышении эффективности реестра за счет использования существующих региональных реестров, а также существующих реестров групп реагирования на компьютерные инциденты и групп реагирования на инциденты в сфере кибербезопасности:

a) если государства, устанавливающие связь, являются членами одной и той же региональной организации, имеющей действующий реестр контактных пунктов, то государства могут связываться друг с другом, используя либо глобальный реестр контактных пунктов, либо реестр контактных пунктов соответствующей региональной организации. Если государства, устанавливающие связь, не являются членами одной и той же региональной организации, государства могут связываться друг с другом, используя глобальный реестр контактных пунктов;

b) если государства уже определились с назначением дипломатических и технических контактных пунктов в другие региональные реестры, рекомендуется, чтобы те же дипломатические и технические контактные пункты были назначены государствами и в глобальный реестр контактных пунктов;

---

[2] Доклад ГПЭ 2021 года (A/76/135), пункт 30 d); и принятая на основе консенсуса резолюция 76/19 Генеральной Ассамблеи.

[3] Доклад ГПЭ 2021 года (A/76/135), пункт 77 b); и принятая на основе консенсуса резолюция 76/19 Генеральной Ассамблеи.

c) в соответствующих случаях УВРООН в консультации с администраторами существующих реестров изучает возможность взаимоусиления на техническом уровне и регулярного обмена обновленной информацией между такими реестрами и глобальным реестром контактных пунктов по соответствующим защищенным каналам связи по согласованию со всеми участниками этого существующего реестра.

**Наращивание потенциала**

13. Руководствуясь содержащейся в первом ежегодном докладе о проделанной работе рекомендацией государствам участвовать в обсуждении инициатив по наращиванию соответствующего потенциала в связи с формированием реестра контактных пунктов, государства соглашаются на разработку специального плана помощи в соответствии с принципами наращивания потенциала, изложенными в приложении C, в который войдут следующие добровольные элементы помощи развивающимся странам в наращивании необходимого технического потенциала для эффективного участия в реестре контактных пунктов:

Действия Секретариата Организации Объединенных Наций

a) Секретариату Организации Объединенных Наций предлагается разработать в партнерстве с заинтересованными государствами онлайн-руководство «Реестр контактных пунктов: вводный курс», посвященное практическим аспектам начала работы с реестром контактных пунктов и участия в нем, с тем чтобы оказать государствам поддержку в назначении национальных контактных пунктов и помочь им в использовании реестра контактных пунктов;

b) Секретариату Организации Объединенных Наций предлагается запросить мнения государств о потенциале, необходимом для участия в реестре контактных пунктов, которые могут включать мнения об опыте наращивания потенциала, полученном при участии в других реестрах контактных пунктов. Исходя из этого, Секретариату Организации Объединенных Наций предлагается не позднее июня 2024 года подготовить первоначальный справочный документ, в котором будут: i) отражены мнения, представленные государствами; ii) определены возможности, необходимые для эффективного участия контактных пунктов в реестре контактных пунктов; и iii) предложены соответствующие меры по наращиванию такого потенциала, включая, в частности, программы, разработанные специально для отобранных контактных пунктов;

c) Секретариату Организации Объединенных Наций при поддержке заинтересованных государств и соответствующих структур предлагается разработать серию специализированных модулей электронного обучения, посвященных потенциалу, необходимому для продуктивного участия контактных пунктов в работе реестра контактных пунктов, о которых говорится в справочном документе Секретариата Организации Объединенных Наций;

Действия РГОС и председателя РГОС

d) на предстоящих сессиях РГОС государствам предлагается принять участие в дальнейших целенаправленных обсуждениях потенциальных последующих мер, опираясь на информацию, представленную в справочном документе Секретариата Организации Объединенных Наций. В ходе этих обсуждений государствам предлагается также проанализировать инициативы, представленные на веб-сайте РГОС в соответствии с пунктами 13 f) и g), и рассмотреть вопрос о том, какие дополнительные инициативы могут потребоваться для наращивания потенциала, указанного в справочном документе Секретариата Организации Объединенных Наций;

e) Председателю РГОС предлагается организовать в партнерстве с заинтересованными государствами испытание имитационной модели с использованием базовых сценариев, позволяющих представителям государств смоделировать практические аспекты участия в реестре контактных пунктов и лучше понять роли дипломатических и технических контактных пунктов;

Действия заинтересованных государств (на добровольной основе)

f) государства могут созывать совещания технических экспертов государств, готовящихся к участию в реестре контактных пунктов, в очном или смешанном формате на субрегиональном, региональном, межрегиональном и глобальном уровнях для обсуждения и обмена опытом, связанным с участием в реестрах контактных пунктов, по линии сотрудничества Юг — Юг, Север — Юг, а также трехстороннего, субрегионального и регионального сотрудничества. Государствам предлагается в кратчайшие сроки сообщать о таких инициативах в Секретариат Организации Объединенных Наций, которому поручено регулярно обобщать и публиковать информацию о них на веб-сайте РГОС;

g) государства и/или группа государств, которые имеют такую возможность, могут поддержать наращивание потенциала в отношении реестра контактных пунктов, в том числе в сотрудничестве, сообразно обстоятельствам, с региональными и субрегиональными организациями и другими заинтересованными сторонами, включая представителей деловых кругов, неправительственных организаций и научно-академического сообщества. Таким государствам предлагается в кратчайшие сроки сообщать об их инициативах в Секретариат Организации Объединенных Наций, которому поручено регулярно обобщать и публиковать информацию о них на веб-сайте РГОС; кроме того, государствам рекомендуется, в соответствующих случаях, в приоритетном порядке рассматривать возможность участия назначенных контактных пунктов в их программах по наращиванию потенциала.

**Дальнейшая работа**

14. Начальный этап введения в действие реестра контактных пунктов должен быть осуществлен в кратчайшие сроки. Дальнейшая доработка реестра контактных пунктов будет происходить поступательно и поэтапно, в соответствии с целями и принципами, изложенными выше. В этой связи государства могли бы одновременно продолжить обсуждение:

a) инициатив по поощрению и расширению добровольного участия государств в реестре контактных пунктов;

b) протоколов связи, включая надлежащую обработку полученной в ходе обмена информации и возможной дальнейшей разработки шаблонов и процедур взаимодействия;

c) дальнейших идей по повышению эффективности функционирования реестра контактных пунктов и улучшению его возможностей в деле содействия связям между государствами;

d) дальнейших усилий по наращиванию потенциала, направленных на обеспечение всестороннего участия государств в реестре контактных пунктов.

15. Председателю РГОС предлагается регулярно созывать очные или виртуальные встречи контактных пунктов, начиная с совещания дипломатических контактных пунктов, за которым последует совещание дипломатических и технических контактных пунктов, для обмена практической информацией и опытом по введению в действие и использованию реестра контактных пунктов.

16. После первоначального введения в действие реестра контактных пунктов государства проведут анализ его работы и, при необходимости, рассмотрят возможности его доработки, в том числе по линии обмена опытом между государствами в вопросах использования реестра контактных пунктов. В связи с этим председателю РГОС предлагается созвать в 2024 году специальное совещание РГОС, чтобы дать возможность государствам-участникам проанализировать введение в действие и имплементацию реестра контактных пунктов и рассмотреть возможности его доработки с учетом целей и принципов реестра контактных пунктов.

## Дополнение к приложению А, озаглавленному «Элементы разработки и введения в действие глобального межправительственного реестра контактных пунктов»

### Процедура запроса

При запросе у другого участника информации об инциденте, связанном с безопасностью в сфере использования ИКТ, контактные пункты могут предпринять следующие шаги:

1. позвонить или написать электронное сообщение соответствующему контактному пункту, указав свои имя, фамилию и представляемую организацию;
2. предоставить как можно более полную информацию о характере инцидента;
3. попросить предоставить дополнительную информацию об инциденте и сообщить свои контактные данные. При необходимости указать степень срочности;
4. указать предпочтительный канал связи и определить ведомство в стране запрашивающего, которое станет основным контактным пунктом по данному конкретному инциденту.

### Процедура ответа на запрос

При ответе на запрос об инциденте, связанном с безопасностью в сфере использования ИКТ, контактные пункты могут предпринять следующие шаги:

1. дать незамедлительный ответ на запрос об инциденте, связанном с безопасностью в сфере использования ИКТ (если это возможно), или:
2. сообщить контактному пункту о необходимости изучить обстоятельства этого инцидента и получить дополнительную информацию. При необходимости указать приблизительные сроки ответа; и
3. согласовать предпочтительный канал связи и определить ведомство в стране отвечающего, которое станет основным контактным пунктом по данному конкретному инциденту.

# Приложение B

## Первоначальный перечень добровольных глобальных мер укрепления доверия

Ниже приводится первоначальный, неисчерпывающий перечень добровольных глобальных мер укрепления доверия (МД). Эти глобальные меры укрепления доверия взяты из заключительного доклада Рабочей группы открытого состава 2021 года, а также первого и второго ежегодных докладов РГОС о проделанной работе. Со временем, по мере необходимости, в этот перечень могут быть добавлены дополнительные глобальные меры укрепления доверия, отражающие результаты обсуждений в рамках РГОС.

### МД 1. Назначение национальных контактных пунктов для включения в глобальный реестр контактных пунктов, а также введение в действие и использование глобального реестра контактных пунктов

a) Государства согласились составить, опираясь на результаты проделанной на региональном уровне работы, глобальный межправительственный реестр контактных пунктов. На четвертой и пятой сессиях РГОС государствам предлагается принять участие в дальнейших целенаправленных обсуждениях вопросов составления такого реестра на основе консенсуса, а также в обсуждении инициатив по наращиванию соответствующего потенциала с учетом, сообразно обстоятельствам, имеющегося передового опыта, такого как опыт на региональном и субрегиональном уровне.

**[Первый ежегодный доклад РГОС о проделанной работе, раздел «Меры укрепления доверия», подраздел «Рекомендуемые дальнейшие действия», пункт 2]**

b) 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.

**[Доклад РГОС 2021 года, пункт 51]**

c) Государствам предлагается ввести в действие и использовать глобальный реестр контактных пунктов, осуществляя следующие действия:

i) проверку связи в виде «пинг-тестов»;

ii) добровольный обмен информацией, в том числе при возникновении требующего безотлагательного внимания или значительного инцидента в сфере использования ИКТ, осуществляемый через глобальный реестр контактных пунктов;

iii) тренировочные занятия для моделирования практических аспектов участия в реестре контактных пунктов;

iv) регулярные очные или виртуальные встречи контактных пунктов для обмена практической информацией и опытом по введению в действие и использованию реестра контактных пунктов на добровольной основе;

v) использование реестра контактных пунктов для установления связи между контактными пунктами в соответствии с порядком работы реестра контактных пунктов.

**МД 2. Продолжение обмена мнениями и проведение двустороннего, субрегионального, регионального, межрегионального и многостороннего диалога и консультаций между государствами**

a) Государства пришли к выводу о том, что диалог в рамках РГОС сам по себе является мерой укрепления доверия, поскольку он стимулирует открытый и транспарентный 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 имплементации рамок ответственного поведения государств при использовании ИКТ.

**[Доклад РГОС 2021 года (A/75/816), пункт 43]**

b) 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.

**[Доклад РГОС 2021 года (A/75/816), пункт 52]**

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

**[Доклад РГОС 2021 года, пункт 53]**

d) Государства вновь подчеркнули, что сама РГОС служит одной из мер укрепления доверия.

**[Первый ежегодный доклад РГОС о проделанной работе, пункт 16 e)]**

**МД 3. Обмен информацией, например, о национальных концептуальных документах по ИКТ, национальных стратегиях, политике и программах, законодательных актах и примерах передового опыта, на добровольной основе**

a) 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.

**[Доклад РГОС 2021 года, пункт 48]**

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

**[Доклад РГОС 2021 года, пункт 50]**

c) Государствам рекомендуется продолжать на добровольной основе обмен концептуальными документами, национальными стратегиями, политическими документами и программами, а также информацией об учреждениях и структурах в сфере ИКТ, имеющих отношение к международной безопасности, в том числе, сообразно обстоятельствам, в рамках доклада Генерального секретаря о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также портала ЮНИДИР по киберполитике.

**[Первый ежегодный доклад РГОС о проделанной работе, раздел «Меры укрепления доверия», подраздел «Рекомендуемые дальнейшие действия», пункт 5]**

### МД 4. Поддержка расширения возможностей для совместной разработки и применения мер укрепления доверия

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

**[Доклад РГОС 2021 года, пункт 49]**

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

**[Доклад РГОС 2021 года, пункт 53]**

c) Государства продолжат в рамках РГОС обмен мнениями о разработке и имплементации мер укрепления доверия, в том числе о возможной разработке дополнительных мер укрепления доверия.

**[Первый ежегодный доклад РГОС о проделанной работе, раздел «Меры укрепления доверия», подраздел «Рекомендуемые дальнейшие действия», пункт 1]**

# Приложение C

## Согласованные принципы наращивания потенциала[1]

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 различных 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.

**Партнерства**

- 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.

[1] В соответствии с достигнутой договоренностью, отраженной в пункте 56 заключительного доклада РГОС 2021 года (A/75/816).

# Приложение D

## Перечень рабочих документов, в которых изложены национальные и групповые позиции, идеи и инициативы

## (Отсортированы по дате подачи, в обратном хронологическом порядке, по состоянию на 27 июля 2023 года)

Рабочий документ о глобальном портале сотрудничества в области кибербезопасности (представлен Индией, новая версия [с изменениями в режиме правки])
**Индия**

Рабочий документ о глобальном портале сотрудничества в области кибербезопасности (представлен Индией, новая версия [с принятыми изменениями])
**Индия**

Применимость международного права, в частности Устава Организации Объединенных Наций, при использовании ИКТ: точки соприкосновения (представлен группой государств)
**Различные государства (Австралия, Колумбия, Сальвадор, Уругвай, Эстония)**

Обновленный проект рабочего документа о создании хранилища информации об угрозах в рамках Организации Объединенных Наций (представлен Кенией)
**Кения**

Документ с изложением позиции по применению международного права в киберпространстве (представлен Коста-Рикой)
**Коста-Рика**

Документ с изложением позиции по применению международного права в киберпространстве (представлен Ирландией)
**Ирландия**

Обновленная концепция конвенции Организации Объединенных Наций об обеспечении международной информационной безопасности (предложение Российской Федерации, соавторы: Беларусь, Венесуэла, КНДР, Никарагуа, Сирия)
**Российская Федерация**

Рабочий документ о применимости международного права, в частности Устава ООН, при использовании ИКТ: точки соприкосновения (представлен группой государств)
**Различные государства (Австралия, Колумбия, Сальвадор, Эстония)**

Материалы для доклада Генерального секретаря, представляемого во исполнение резолюции 77/37 Генеральной Ассамблеи ООН (представлены Францией)
**Франция**

Рабочий документ о пробном введении в действие реестра контактных пунктов (представлен Ираном (Исламская Республика))
**Иран (Исламская Республика)**

Проект рабочего документа о создании хранилища информации об угрозах в рамках ООН (представлен Кенией)
**Кения**

Использование реестра контактных пунктов ООН по кибербезопасности: связь, обмен информацией и проведение испытаний (представлен Германией от имени группы государств)
**Различные государства (Австралия, Аргентина, Бразилия, Германия, Израиль, Канада, Кения, Мексика, Нидерланды, Республика Корея, Сингапур, Фиджи, Чешская Республика, Чили, Уругвай)**

Документ с изложением мнений о будущем регулярном институциональном диалоге по ИКТ в контексте международной безопасности (представлен Бразилией)
**Бразилия**

Мера укрепления доверия № 1 о формировании глобального межправительственного реестра контактных пунктов (предложение Российской Федерации, соавторы: Беларусь, Никарагуа)
**Российская Федерация**

Концептуальный документ Российской Федерации по организации под эгидой Организации Объединенных Наций регулярного институционального диалога с участием всех государств — членов ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ (соавторы: Беларусь, Никарагуа)
**Российская Федерация**

Рабочий документ о глобальном портале сотрудничества в области кибербезопасности (представлен Индией)
**Индия**

Рабочий документ о сфере охвата, структуре и содержании предлагаемой программы действий по поощрению ответственного поведения государств при использовании ИКТ в контексте международной безопасности (представлен Египтом)
**Египет**

Документ с изложением позиции по применению международного права в киберпространстве (представлен Пакистаном)
**Пакистан**

Концептуальный документ о глобальном реестре контактных пунктов (представлен Венесуэлой)
**Венесуэла (Боливарианская Республика)**

Документ с изложением позиции по формированию глобального реестра контактных пунктов (представлен Иорданией)
**Иордания**

Документ с изложением мнения о формировании глобального реестра контактных пунктов (представлен Испанией)
**Испания**

Документ с изложением мнений о реестре контактных пунктов (представлен Мексикой)
**Мексика**

Документ с изложением мнений о глобальном реестре контактных пунктов, представленный в соответствии с первым ежегодным докладом о проделанной работе, содержащимся в документе A/77/275 (представлен Эстонией)
**Эстония**

Документ с изложением мнения о формировании глобального реестра контактных пунктов (представлен Словакией)
**Словакия**

Документ с изложением предварительных мнений о глобальном реестре контактных пунктов (представлен Венгрией)
**Венгрия**

Материалы о глобальном реестре контактных пунктов, представленные в соответствии с документом A/77/275 (представлены Марокко)
**Марокко**

Документ с изложением мнения о глобальном реестре контактных пунктов (представлен Республикой Корея)
**Республика Корея**

Документ с изложением национальных мнений о глобальном реестре контактных пунктов (представлен Арменией)
**Армения**

Материалы о глобальном реестре контактных пунктов (представлены Мексикой)
**Мексика**

Материалы для справочного документа по глобальному реестру контактных пунктов (представлены Сенегалом)
**Сенегал**

Документ с изложением мнения о реестре контактных пунктов в Организации Объединенных Наций (представлен Сингапуром)
**Сингапур**

Документ с изложением мнения о формировании глобального реестра контактных пунктов (представлен Пакистаном)
**Пакистан**

Документ с изложением мнения о глобальном реестре контактных пунктов, представленный в соответствии с документом A/77/275 (представлен Чешской Республикой)
**Чешская Республика**

Документ с изложением позиции по глобальному реестру контактных пунктов (представлен Египтом)
**Египет**

Документ с изложением мнения о глобальных сети и реестре контактных пунктов по безопасности в сфере ИКТ (представлен Италией)
**Италия**

Создание реестра контактных пунктов (представлен Индией)
**Индия**

Документ с изложением национального мнения о глобальном реестре национальных контактных пунктов (представлен Сальвадором)
**Сальвадор**

Документ с изложением предварительной позиции и рекомендаций по глобальному реестру контактных пунктов (представлен Румынией)
**Румыния**

Документ с изложением мнений о глобальном реестре контактных пунктов, представленный в соответствии с документом A/77/275 (представлен Соединенным Королевством)
**Соединенное Королевство**

Документ с изложением мнения о формировании глобального реестра контактных пунктов по кибербезопасности (представлен Францией)
**Франция**

Реализация мер на глобальном уровне по обеспечению доверия в киберпространстве: на пути к реестру контактных пунктов (представлен Германией от имени группы государств)
**Различные государства (Австралия, Бразилия, Германия, Израиль, Канада, Мексика, Нидерланды, Республика Корея, Сингапур, Фиджи, Чили и Уругвай)**

Материалы для справочного документа по реестру контактных пунктов (представлены Южной Африкой)
**Южная Африка**

Документ с изложением мнений о глобальном реестре контактных пунктов (представлен Малайзией)
**Малайзия**

Материалы о глобальном реестре контактных пунктов (представлены Колумбией)
**Колумбия**

Материалы для справочного документа по глобальному реестру контактных пунктов (представлены Германией)
**Германия**

Неофициальный документ о создании глобального межправительственного реестра контактных пунктов (представлен Китаем)
**Китай**

Концептуальный документ о функциональной эквивалентности как важнейшем элементе эффективного функционирования контактных пунктов (представлен Ираном (Исламская Республика))
**Иран (Исламская Республика)**

Концептуальный документ о формировании реестра контактных пунктов (представлен Российской Федерацией)
**Российская Федерация**

Обновленный концептуальный документ о практическом подходе к международному праву (представлен Канадой и Швейцарией)
**Различные государства (Канада и Швейцария)**

Концептуальная записка о мерах укрепления доверия (представлена Германией от имени группы государств)
**Германия**

Концептуальный документ Российской Федерации о формировании реестра контактных пунктов
**Российская Федерация**

Наращивание потенциала (предложение Колумбии)
**Колумбия**

Меры укрепления доверия (совместное предложение Австралии, Бразилии, Германии, Израиля, Канады, Мексики, Нидерландов, Республики Корея, Сингапура)
**Различные государства (Австралия, Бразилия, Германия, Израиль, Канада, Мексика, Нидерланды, Республика Корея и Сингапур)**

Совместное предложение к разделу об угрозах первого ежегодного доклада о проделанной работе (представлено Австралией, Ботсваной, Данией, Индонезией, Коста-Рикой, Малайзией, Нидерландами, Соединенным Королевством, Чили)
**Различные государства (Австралия, Ботсвана, Дания, Индонезия, Коста-Рика, Малайзия, Нидерланды, Соединенное Королевство и Чили)**

Глобальный портал сотрудничества в области кибербезопасности: концептуальная записка
**Индия**

Совместные поправки к ежегодному докладу о проделанной работе (представлены Боливией, Венесуэлой, Кубой, Никарагуа)
**Различные государства (Боливия, Венесуэла, Куба, Никарагуа)**

Документ с изложением совместной позиции по проекту ежегодного доклада о проделанной работе
**Различные государства (Республика Беларусь, Боливарианская Республика Венесуэла, Республика Куба, Исламская Республика Иран, Республика Никарагуа, Российская Федерация и Сирийская Арабская Республика)**

Введение и существующие и потенциальные угрозы: комментарии и предложения по тексту (представлены Нидерландами)
**Нидерланды**

Предложения по тексту первого ежегодного доклада о проделанной работе: введение, раздел об угрозах и раздел о нормах (представлены Австралией)
**Австралия**

Совместный рабочий документ о формировании сети контактных пунктов ООН по кибербезопасности (представлен группой государств)
**Различные государства (Австралия, Бразилия, Германия, Израиль, Канада, Мексика, Нидерланды, Республика Корея и Сингапур**)

Документ с изложением позиции по применению международного права в киберпространстве (представлен Швецией)
**Швеция**

Модель развитости потенциала кибербезопасности: оценка основных потребностей и национальные стратегии (представлена несколькими государствами)
**Различные государства (Австралия, Белиз, Ботсвана, Вануату, Германия, Грузия, Доминиканская Республика, Исландия, Колумбия, Маврикий, Малави, Нидерланды, Норвегия, Парагвай, Перу, Руанда, Соединенное Королевство, Танзания, Швейцария, Уганда, Фиджи, Чили, Эквадор, Япония**)

Продвижение глобальной программы действий в области кибербезопасности: варианты и приоритеты (представлен Канадой)
**Канада**

Практический подход к международному праву в работе РГОС 2021-2025 (представлен Канадой и Швейцарией)
**Различные государства (Канада и Швейцария**)

Рабочий документ, направленный на развитие продолжающихся обсуждений в рамках РГОС ООН по мерам укрепления доверия в киберпространстве
**Различные государства**

Программа тренировочных занятий ООН для национальных контактных пунктов по киберпространству (представлена Сингапуром)
**Сингапур**

Концептуальная записка о совместной стипендиальной программе Организации Объединенных Наций и Сингапура по кибербезопасности (представлена Сингапуром)
**Сингапур**

Международное право, применимое к деятельности в киберпространстве (представлен Канадой)
**Канада**

Российские поправки к проекту доклада РГОС от 22 июня 2022 года
**Российская Федерация**

Предложение Канады по работе РГОС по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025
**Канада**

Документ с изложением позиции Китая по разработке международных правил в киберпространстве
**Китай**

Глобальная инициатива по безопасности данных (представлена Китаем)
**Китай**

Документ, представленный к первой основной сессии (представлен Ираном (Исламская Республика))
**Иран (Исламская Республика)**

Международное право, применимое к деятельности в киберпространстве (представлен Францией)
**Франция**

Документ с изложением мнений Китая о применении принципа суверенитета в киберпространстве
**Китай**

Документ с изложением позиции Эстонии: РГОС ООН 2021–2025: достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности
**Эстония**

Рабочий документ о программе действий по поощрению ответственного поведения государств при использовании ИКТ (представлен группой государств)
**Различные государства (Австралия, Австрия, Аргентина, Бельгия, Болгария, Венгрия, Габон, Гватемала, Германия, Греция, Грузия, Дания, Египет, Ирландия, Исландия, Испания, Италия, Канада, Республика Кипр, Колумбия, Латвия, Ливан, Литва, Лихтенштейн, Люксембург, Мальта, Марокко, Монако, Нидерланды, Норвегия, Объединенные Арабские Эмираты, Польша, Португалия, Республика Корея, Республика Молдова, Румыния, Сальвадор, Республика Северная Македония, Сингапур, Словакия, Словения, Соединенное Королевство, Украина, Финляндия, Франция, Хорватия, Черногория, Чешская Республика, Чили, Швейцария, Швеция, Эквадор, Эстония, Япония)**

Документ с изложением позиции Италии по международному праву и киберпространству
**Италия**

Концепция деятельности Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 (представлена Российской Федерацией)
**Российская Федерация**

Применение международного права в киберпространстве (представлен Германией)
**Германия**

Предложения Российской Федерации по правилам, нормам и принципам ответственного поведения государств в информационном пространстве
**Российская Федерация**