Организация Объединенных Наций A/79/214*

Генеральная Ассамблея

Distr.: General
22 July 2024
Russian
Original: English

Семьдесят девятая сессия
Пункт 93 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 третий ежегодный доклад о проделанной работе, представленный рабочей группой открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025.

* Переиздано по техническим причинам 2 октября 2024 года.
** A/79/150.

24-13414* (R) 090924 021024

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. Второй ежегодный доклад рабочей группы о проделанной работе, посвященный ее четвертой и пятой основным сессиям, был опубликован в виде документа A/78/265.

II. Организационные вопросы

A. Открытие и продолжительность шестой, седьмой и восьмой основных сессий

3. Рабочая группа провела свою шестую основную сессию 11–15 декабря 2023 года, свою седьмую основную сессию 4–8 марта 2024 года и свою восьмую основную сессию 8–12 июля 2024 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 шестой, седьмой и восьмой основных сессий приводится в документах A/AC.292/2023/INF/7, A/AC.292/2024/INF/2 и A/AC.292/2024/INF/4 соответственно.

C. Должностные лица

6. На шестой, седьмой и восьмой основных сессиях рабочей группы Председателем являлся г-н Бурхан Гафур (Сингапур).

D. Организация работы

7. На 1-м заседании шестой основной сессии 11 декабря 2023 года рабочая группа согласовала порядок организации своей работы, изложенный в документе A/AC.292/2023/4. Она также одобрила участие в ее работе неправительственных структур, перечисленных в документе A/AC.292/2023/INF/6.

8. На 1-м заседании седьмой основной сессии 4 марта 2024 года рабочая группа согласовала порядок организации своей работы, изложенный в документе A/AC.292/2024/1. Она также одобрила участие в ее работе неправительственных структур, перечисленных в документе A/AC.292/2024/INF/1.

9. На 1-м заседании восьмой основной сессии 8 июля 2024 года рабочая группа согласовала порядок организации своей работы, изложенный в документе A/AC.292/2024/4. Она также одобрила участие в ее работе неправительственных структур, перечисленных в документе A/AC.292/2024/INF/3.

E. Документация

10. 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

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

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

13. На своей восьмой основной сессии в ходе девяти пленарных заседаний рабочая группа рассмотрела пункты 3, 5, 6 и 7 повестки дня.

14. 13–17 мая и 1 июля 2024 года Председатель, руководствуясь решениями 77/512 и 78/541 Ассамблеи, созывал специальные межсессионные совещания для заслушивания 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), и в ходе этих совещаний эксперты из представленного делегациями списка назначенных экспертов провели брифинги по отдельным темам с участием заинтересованных сторон.

15. 9 мая 2024 года Председатель созвал первое совещание представителей контактных пунктов из глобального реестра контактных пунктов в соответствии с документом A/78/265 и решением 78/541 Генеральной Ассамблеи. Это первое совещание представителей контактных пунктов также ознаменовало официальное начало использования глобального реестра контактных пунктов.

16. В соответствии с решением 78/541 Генеральной Ассамблеи 10 мая 2024 года Председатель созвал первый глобальный круглый стол высокого уровня по вопросам наращивания потенциала в области безопасности информационно-коммуникационных технологий, чтобы обеспечить специалистам-практикам в области наращивания потенциала, представителям государств и заинтересованным сторонам платформу для обмена идеями и передовым опытом и налаживания партнерских отношений с целью расширения взаимодействия и продвижения работы международного сообщества по наращиванию потенциала конкретными способами.

17. 28 сентября 2023 года и 31 января, 27 марта и 10 июня 2024 года Председатель созывал виртуальные неофициальные заседания, чтобы провести брифинги для делегаций по аспектам, рассматриваемым рабочей группой.

18. 13 декабря 2023 года и 6 марта и 10 июля 2024 года в соответствии с согласованным порядком участия заинтересованных сторон в ходе 6-го заседания шестой основной сессии, 6-го заседания седьмой основной сессии и 5-го заседания восьмой основной сессии были проведены специальные заседания заинтересованных сторон.

19. 6 декабря 2023 года и 28 февраля и 3 июля 2024 года Председатель провел неофициальные консультативные обсуждения с заинтересованными сторонами, включая представителей деловых кругов, неправительственных структур и научных кругов, 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

20. На своей восьмой основной сессии рабочая группа рассмотрела 12 июля 2024 года пункт 7 повестки дня, озаглавленный «Утверждение ежегодных докладов о проделанной работе», и утвердила проект доклада рабочей группы открытого состава (A/AC.292/2024/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.292/2024/CRP.1 (см. приложение).

21. Подборка заявлений с разъяснением позиций будет издана в качестве документа A/AC.292/2024/INF/5.

Приложение*

Доклад о ходе обсуждения рабочей группой пункта 5 повестки дня

A. Общий обзор

1. Шестая, седьмая и восьмая официальные сессии, а также специальные 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, которое 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 напомнили далее 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 подготовленное Председателем резюме и неисчерпывающий перечень предложений, содержащийся в приложении к подготовленному Председателем резюме, 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 и второй консенсусные ежегодные доклады 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[7] ответственного поведения государств в области использования ИКТ, выступая в качестве основы работы нынешней РГОС и будущих постоянных механизмов.

---

* Публикуется без официального редактирования.

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

[2] A/75/816.

[3] A/76/135.

[4] A/77/275 и A/78/265 соответственно.

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

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

[7] Доклад ГПЭ 2021 года (A/76/135), п. 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 уделять должное внимание как дальнейшему содействию достижению государствами общего понимания в вопросах безопасности в сфере использования ИКТ, так и дальнейшему выполнению существующих обязательств.

5. По мере того, как дискуссии в рамках РГОС приобретают все более глубокий характер, государства все чаще признают взаимосвязь между всеми вопросами, рассматриваемыми в рамках РГОС. В этой связи государства подчеркнули, что работа РГОС, а затем и будущего постоянного механизма будет носить комплексный, стратегически ориентированный и межсекторальный характер.

6. 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 имеет существенно важное значение. В связи с этим возникает необходимость выработки устойчивых, эффективных и доступных решений.

7. РГОС далее подчеркнула, что наращивание потенциала имеет основополагающее значение для развития ресурсов, навыков, стратегий и институциональных структур, необходимых для повышения степени устойчивости и безопасности ИКТ в государствах, а также для ускорения процесса цифрового преобразования государств и осуществления Повестки дня в области устойчивого развития на период до 2030 года. Государства далее признали, что наращивание потенциала способствует укреплению рамок ответственного поведения государств в области использования ИКТ и способствует формированию открытой, безопасной, надежной, стабильной, доступной, мирной и взаимосовместимой ИКТ-среды. В свете ускоренного формирования цифрового ландшафта необходимо активизировать усилия по наращиванию потенциала с учетом потребностей, что станет одной из ключевых функций будущего постоянного механизма, в целях преодоления цифрового разрыва и обеспечения всем государствам возможности безопасно и надежно использовать блага цифровых технологий. В этой связи государства подтвердили принципы наращивания потенциала в сфере обеспечения безопасности ИКТ, принятые в докладе РГОС 2021 года и изложенные во втором ежегодном докладе о проделанной работе.

8. 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 1-м 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 научного сообщества[8].

9. РГОС признала, что региональные и субрегиональные организации могли бы и далее 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 региональных организаций и не все региональные организации делают упор на вопросы безопасности в области использования ИКТ, РГОС отметила, что прилагаемые на региональном уровне усилия служат дополнением к ее работе[9].

10. РГОС с удовлетворением отметила высокий уровень участия женщин-делегатов в работе ее сессий и тот факт, что в ходе проводимых ею обсуждений гендерным аспектам уделяется большое внимание. РГОС подчеркнула важность сокращения «гендерного цифрового разрыва» и содействия обеспечению всестороннего, равноправного и конструктивного участия и лидерства женщин в процессах принятия решений, связанных с использованием ИКТ в контексте международной безопасности.

11. Настоящий третий ежегодный доклад о проделанной работе содержит информацию о конкретных действиях и совместных мерах по противодействию угрозам в сфере ИКТ и по содействию созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды и в этом отношении опирается на первый и второй ежегодные доклады о проделанной работе, одобренные консенсусом в решениях 77/512 и 78/541 Генеральной Ассамблеи. В знак признания того, что в РГОС ведутся непрерывные обсуждения и что субстантивные обсуждения в ходе работы РГОС будут проводиться до завершения ее мандата в 2025 году, настоящий третий ежегодный доклад о проделанной 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 и втором ежегодных докладах о проделанной работе. Во исполнение мандата РГОС, определенного в резолюции 75/240, настоящий третий доклад о проделанной работе будет представлен Генеральной Ассамблее.

B. Существующие и потенциальные угрозы

12. В ходе шестой, седьмой и восьмой сессий, а также специальных межсессионных совещаний 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 именно под этим углом. Напомнив об угрозах, отмеченных в первом и втором ежегодном докладе о проделанной работе, докладе РГОС 2021 года и докладах ГПЭ, государства вновь указали, что

[8] Первый ежегодный доклад о проделанной работе, п. 4, и второй ежегодный доклад о проделанной работе, п. 6.

[9] Первый ежегодный доклад о проделанной работе, п. 5, и второй ежегодный доклад о проделанной работе, п. 7.

они все более обеспокоены тем, что в нынешней по-прежнему сложной геополитической обстановке угрозы, связанные с использованием ИКТ в контексте международной безопасности, усилились и существенным образом изменились.

13. Государства напомнили о том, что ряд государств занимается наращиванием потенциала в сфере ИКТ для военных целей. Они напомнили также, что применение ИКТ в будущих конфликтах между государствами становится все более вероятным, и отметили, что ИКТ уже применяются в конфликтах в различных регионах. Дальнейшее 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 в сфере ИКТ, которые ранее были доступны только государствам[10].

14. Государства выразили обеспокоенность наращиванием злонамеренной деятельности в сфере ИКТ, которая затрагивает критически важную инфраструктуру (КВИ) и критически важную информационную инфраструктуру (КВИИ), в частности здравоохранение, морское судоходство, авиацию, финансовый и энергетический секторы. Потенциально такие КВИ и КВИИ могут обеспечивать предоставление существенно важных услуг, выходящих за пределы границ и юрисдикций, и атаки на них с помощью ИКТ могут иметь каскадные последствия на национальном, региональном и глобальном уровнях[11]. Государства подчеркнули, что определение инфраструктур, которые они относят к категории критически важных, является прерогативой каждого государства[12].

15. Государства подчеркнули, что злонамеренные действия с использованием ИКТ, направленные против КВИ и КВИИ и подрывающие доверие в отношениях между государствами, а также доверие к политическим и избирательным процессам и государственным институтам или оказывающие влияние на общедоступность и целостность интернета, вызывают реальную и растущую озабоченность[13].

16. Государства особо отметили необходимость защиты подводных кабелей и орбитальных систем связи от злонамеренных действий, которые могли бы нанести значительный ущерб телекоммуникационным сетям или нарушить их работу и потенциально повлиять на функционирование технической инфраструктуры, имеющей существенно важное значение для обеспечения доступности и целостности интернета в больших районах земного шара.

17. Кроме того, государства выразили обеспокоенность по поводу злонамеренной деятельности в сфере ИКТ, направленной против международных организаций и гуманитарных организаций, поскольку такая деятельность может повлиять на способность этих организаций выполнять их соответствующие мандаты безопасным, надежным и независимым образом и подорвать доверие к их работе.

18. Государства с тревогой отметили активизацию злонамеренного использования государствами скрытых информационных кампаний с применением ИКТ для оказания влияния на процессы, системы и общую стабильность других государств. Такие действия подрывают доверие, могут потенциально привести к

[10] Доклад РГОС 2021 года (A/75/816), приложение I, п. 16; второй ежегодный доклад о проделанной работе, п. 11.

[11] Второй ежегодный доклад о проделанной работе, п. 12.

[12] Доклад РГОС 2021 года (A/75/816), п. 18.

[13] Доклад РГОС 2021 года (A/75/816), приложение I, п. 18; второй ежегодный доклад о проделанной работе, п. 13.

эскалации ситуации и угрожать международному миру и безопасности. Кроме того, они могут приносить прямой и косвенный вред людям[14]. Особую озабоченность государства выразили по поводу злонамеренной деятельности в сфере ИКТ, направленной на вмешательство во внутренние дела государств[15].

19. Государства выразили озабоченность по поводу злоупотребления уязвимостями ИКТ-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 со стороны ИКТ[16].

20. Государства особо отметили опасность, которую представляют такие вредоносные программы, как вирусы-вымогатели, программы-стиратели и троянские программы, и такие методы, как фишинг, атаки с применением технологии «незаконный посредник» и распределенные атаки типа «отказ в обслуживании» (DDoS). Особую обеспокоенность вызвали атаки с использованием вирусов-вымогателей, совершаемые все большим числом злоумышленников и в разных регионах мира, чему отчасти способствует доступность услуг по организации атак с использованием вирусов-вымогателей. Государства далее с обеспокоенностью отметили, что все более частые, масштабные и серьезные атаки с использованием вирусов-вымогателей причиняют вред, нарушают работу основных служб, предоставляющих услуги населению, и могут повлиять на международный мир и безопасность. Государства отметили необходимость комплексного противодействия всем элементам угрозы применения вирусов-вымогателей, в том числе путем преследования участников операций с их применением, пресечения использования и распространения соответствующего вредоносного программного обеспечения, а также противодействия незаконному финансированию в поддержку их деятельности. Кроме того, государства с беспокойством отметили увеличение числа краж криптовалюты и случаев финансирования злонамеренной деятельности в сфере ИКТ с использованием криптовалюты, что потенциально могло бы повлиять на международную безопасность.

21. Государства отметили расширение рынка коммерчески доступных интрузивных ИКТ-средств и использования уязвимостей в аппаратно-программных комплексах, в том числе в темной паутине. Государства выразили обеспокоенность тем, что доступность таких средств для государственных и негосударственных субъектов расширяет возможности их незаконного и злонамеренного использования и потенциально затрудняет деятельность по смягчению угроз, которые они представляют, и защиту от таких угроз, подчеркнув при этом, что такие средства могли бы использоваться в соответствии с нормами международного права. Государства далее выразили обеспокоенность тем, что распространение интрузивных ИКТ-средств государственными и негосударственными субъектами может стать фактором непреднамеренной эскалации и угрожать международному миру и безопасности.

22. Государства отметили, что технологии сами по себе носят нейтральный характер, а такие новые и новейшие технологии, как искусственный интеллект (ИИ) и квантовые вычисления, расширяют возможности для развития. В то же время их постоянно меняющиеся свойства и характеристики могут потенциально повлиять на использование ИКТ в контексте международной безопасности, создавая новые векторы и уязвимости в пространстве ИКТ. Кроме того, такие технологии могли бы повысить оперативность и расширить потенциал

[14] Второй ежегодный доклад о проделанной работе, п. 14.
[15] Второй ежегодный доклад о проделанной работе, п. 13.
[16] Второй ежегодный доклад о проделанной работе, п. 15.

целевого воздействия, которым обладает злонамеренная деятельность в сфере ИКТ[17]. Существует также вероятность усиления рисков в результате пересечения новых технологий.

23. Государства выразили особую обеспокоенность по поводу безопасности и защищенности систем ИИ, а также данных, используемых для подготовки моделей машинного обучения и ИИ, которые применяются в контексте обеспечения безопасности ИКТ. ИИ может использоваться для усиления безопасности ИКТ, повышения устойчивости, улучшения времени реагирования на инциденты в сфере ИКТ и укрепления сетей. Кроме того, государства подчеркнули, что использование ИИ, вероятно, приведет к увеличению числа и усилению воздействия нападений с применением ИКТ в результате развития и совершенствования существующих тактики, методов и процедур. Такие операции могут повысить риск каскадных эффектов, которые могут причинить непреднамеренный вред, в том числе людям и критически важной инфраструктуре. В этой связи государства подчеркнули, что необходимо лучше понимать риски, связанные с новыми и новейшими технологиями, включая ИИ, с точки зрения их роли в обеспечении безопасности ИКТ, а также обеспечивать и усиливать безопасность на протяжении всего жизненного цикла этих технологий, с тем чтобы в полной мере использовать возможности, открывающиеся благодаря таким технологиям. Государства подчеркнули также, что поощрение использования новых и новейших технологий в мирных целях отвечает интересам всех государств.

24. Кроме того, государства отметили возрастающую актуальность защиты данных и обеспечения их безопасности, учитывая увеличение объема и агрегирование данных, связанных с новыми и новейшими технологиями[18].

25. Государства с озабоченностью отметили, что серьезным вызовом становится обеспечение защиты от злонамеренного использования уязвимостей в операционных технологиях и взаимосвязанных вычислительных устройствах, платформах, машинах или объектах, составляющих интернет вещей.

26. Государства вновь 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 не все в равной степени пользуются преимуществами цифровых технологий, и в этой связи отметили необходимость уделения должного внимания растущему цифровому разрыву в контексте ускорения деятельности по осуществлению Повестки дня в области устойчивого развития на период до 2030 года, учитывая при этом национальные потребности и задачи первостепенной важности государств[19].

27. Государства напомнили, что любое использование ИКТ государствами в нарушение их обязательств в соответствии с рамками ответственного поведения государств в области использования ИКТ, включающими добровольные нормы, нормы международного права и меры укрепления доверия, подрывает международный мир и безопасность, доверие и стабильность в отношениях между государствами[20].

---

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

[18] Второй ежегодный доклад о проделанной работе, п. 17.

[19] Второй ежегодный доклад о проделанной работе, п. 18.

[20] Второй ежегодный доклад о проделанной работе, п. 19.

28. Государства вновь выразили обеспокоенность тем, что недостаточная информированность о существующих и потенциальных угрозах и отсутствие надлежащего потенциала для выявления злонамеренных действий с использованием ИКТ, защиты от таких действий и реагирования на них могут привести к повышению их уязвимости[21]. Учитывая меняющуюся картину угроз, связанных с использованием ИКТ в контексте международной безопасности, и принимая во внимание тот факт, что от таких угроз не защищено ни одно государство, государства подчеркнули, что необходимо в срочном порядке повышать степень информированности о таких угрозах и углублять их понимание, а также продолжать разработку и осуществление совместных мер[22] и инициатив по наращиванию потенциала в соответствии с кумулятивными и эволюционирующими рамками ответственного поведения государств[23].

Рекомендуемые дальнейшие действия

29. **Государствам рекомендуется продолжить обмен мнениями в рамках РГОС о существующих и потенциальных угрозах безопасности в сфере использования ИКТ с учетом пунктов 12–28 выше и продолжить целенаправленные обсуждения 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.**

30. **Государствам предлагается представить рабочие документы о возможных способах повышения степени осведомленности о существующих и потенциальных угрозах и углубления их понимания, а также определить возможные совместные меры и инициативы по наращиванию потенциала, которые позволят государствам выявлять такие угрозы, защищаться от них или реагировать на них. Секретариату Организации Объединенных Наций предлагается публиковать эти документы на веб-сайте РГОС, чтобы все государства могли с ними ознакомиться и чтобы РГОС могла продолжить их рассмотрение на ее предстоящих основных сессиях.**

C. Правила, нормы и принципы ответственного поведения государств

31. В ходе шестой, седьмой и восьмой сессий, а также специальных межсессионных совещаний РГОС государства продолжили обсуждение правил, норм и принципов ответственного поведения государств. Государства подтвердили значение кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ и выступили с конкретными, ориентированными на практические действия предложениями в отношении правил, норм и принципов. Ниже приводится неисчерпывающий перечень предложений, которые были в той или иной степени поддержаны государствами и которые могут быть доработаны и дополнены на предстоящих сессиях РГОС:

a) 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 степени

[21] Доклад РГОС 2021 года (A/75/816), приложение I, п. 20.
[22] Доклад РГОС 2021 года (A/75/816), приложение I, п. 22.
[23] Второй ежегодный доклад о проделанной работе, п. 20.

предсказуемости и уменьшении риска заблуждений, 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[24];

b) как предусмотрено нормой c)[25], государства по-прежнему признают, что государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ, и будут приветствовать проведение дальнейших обсуждений для продолжения работы по формированию общего понимания путем обмена национальным и региональным опытом в этой области;

c) как предусмотрено нормами f)[26] и g)[27], 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[28];

d) с учетом сказанного выше 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. Государства подчеркнули, что конкретные меры по защите КВИ и КВИИ могут включать добровольную категоризацию КВИ и КВИИ[29], комплексные оценки рисков, информирование и обучение в области ИКТ, а также разработку соответствующих национальных нормативных требований и руководящих принципов. Государства подчеркнули, что определение инфраструктур, которые они относят к категории критически важных, является прерогативой каждого государства[30]. Государства особо отметили необходимость формирования культуры постоянного совершенствования в целях адаптации к меняющимся ИКТ-угрозам для КВИ и КВИИ. Государства признали также, что

---

[24] Доклад РГОС 2021 года (A/75/816), приложение I, пп. 64 и 65; второй ежегодный доклад о проделанной работе, п. 23 b).

[25] Норма c): Государствам не следует заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ.

[26] Норма f): Государства не должны заведомо осуществлять и поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит их обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения.

[27] Норма 13 g): Государства должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи.

[28] Доклад ГПЭ 2021 года (A/76/135), п. 42; принятая на основе консенсуса резолюция 76/19 Генеральной Ассамблеи; второй ежегодный доклад о проделанной работе, п. 23 c).

[29] Государства подчеркнули, что определение инфраструктур, которые они относят к категории критически важных, является прерогативой каждого государства (доклад РГОС 2021 года (A/75/816), п. 18).

[30] Доклад РГОС 2021 года (A/75/816), п. 18.

наращивание потенциала может помочь операторам КВИ и КВИИ в этом отношении;

e) как указывается в норме i)[31], государства продолжали особо отмечать, что сотрудничество и оказание помощи можно активизировать 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 обеспечению выбора, а также принятие таких совместных мер, 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 применение других подходов, направленных на снижение уровня уязвимости каналов поставок[32];

f) государства подчеркнули также, что в процессе разработки и производства ИКТ-продуктов следует учитывать принцип обеспечения защиты данных на этапе проектирования и соотносить интересы обеспечения защиты и оперативности вывода продукта на рынок;

g) государства вновь 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. Государства далее подчеркнули, что государственно-частные партнерства имеют решающее значение для разработки и продвижения передовых методов обеспечения целостности цепочки поставок, и призвали поддерживать обмен информацией и примерами передовой практики между государствами, а также с участием соответствующих заинтересованных сторон. 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[33];

h) государства подтвердили, что важно поддерживать и продолжать усилия по осуществлению на глобальном, региональном и национальном уровнях норм, которыми соглашаются руководствоваться государства[34];

i) государства приняли к сведению добровольный контрольный перечень практических действий по реализации добровольных, не имеющих обязательной силы норм ответственного поведения государств при использовании ИКТ, содержащийся в приложении A к настоящему докладу. Государства предложили рассматривать контрольный перечень как «живой документ», который можно было бы и далее обсуждать и обновлять на предстоящих сессиях РГОС.

---

[31] Норма i): Государства должны принимать разумные меры для обеспечения целостности каналов поставок, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование скрытых вредоносных функций.

[32] Второй ежегодный доклад о проделанной работе, п. 23 d).

[33] Второй ежегодный доклад о проделанной работе, п. 23 e).

[34] Доклад РГОС 2021 года (A/75/816), п. 27.

В этой связи при использовании этого контрольного перечня следует учитывать различия в уровне технического развития государств, разнообразие национальных систем и региональную специфику. Государства признали также рекомендации по осуществлению, содержащиеся в докладе ГПЭ 2021 года[35], и далее отметили, что существуют и другие доступные ресурсы, которые могли бы помочь государствам в осуществлении существующих правил, норм и принципов. В то же время государства признали, что универсального решения в процессе осуществления не существует;

j) государства напомнили мандат РГОС, содержащийся в резолюции 75/240 Генеральной Ассамблеи, в частности фразу «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»[36];

k) государства подтвердили, что с учетом уникальных особенностей ИКТ со временем можно было бы продолжить разработку дополнительных норм. Кроме того, государства пришли к выводу о том, что дальнейшее развитие норм и применение существующих норм не являются взаимоисключающими, а могут происходить одновременно[37]. В этой связи было выдвинуто несколько предложений относительно возможных новых норм, которые до сих пор обсуждаются государствами;

l) в этой связи государства предложили продолжить обсуждение неисчерпывающего перечня предложений относительно разработки правил, норм и принципов ответственного поведения государств (доклад РГОС 2021 года, приложение к резюме, подготовленному Председателем) в соответствии с рекомендацией, содержащейся в докладе РГОС 2021 года. Государства предложили также, чтобы нынешняя РГОС продолжила обсуждение вопроса о возможной разработке дополнительных норм.

Рекомендуемые дальнейшие действия

32. **Государствам рекомендуется продолжить в рамках РГОС обмен мнениями о правилах, нормах и принципах ответственного поведения государств при использовании ИКТ с учетом подпунктов 31 a)–l) выше на предстоящих основных сессиях РГОС.**

33. **Государствам рекомендуется и далее прилагать усилия по внедрению норм, обсуждать и обновлять добровольный контрольный перечень практических действий (приложение A), который является «живым документом», с целью согласования консенсусной рекомендации по этому добровольному контрольному списку к июлю 2025 года.**

34. **Государствам рекомендуется продолжить обсуждение возможных дополнительных норм ответственного поведения государств при использовании ИКТ на предстоящих сессиях РГОС с опорой на обсуждения, состоявшиеся на предыдущих сессиях РГОС.**

[35] A/76/135.

[36] Резолюция 75/240 Генеральной Ассамблеи, п. 1 постановляющей части; второй ежегодный доклад о проделанной работе, п. 23 a).

[37] Доклад РГОС 2021 года (A/75/816), п. 29.

D. Международное право

35. В ходе шестой, седьмой и восьмой сессий, а также специальных межсессионных совещаний РГОС государства, подтвердив значение кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ, а также подтвердив, что нормы международного права, в частности Устав Организации Объединенных Наций, применимы и существенно важны для поддержания мира, безопасности и стабильности и содействия созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды, продолжили обсуждение вопроса о том, как нормы международного права применяются к использованию ИКТ. РГОС провела целенаправленное углубленное обсуждение тем из неисчерпывающего перечня, приведенного в подпунктах 29 a) и b) второго ежегодного доклада о проделанной работе, а также, в соответствующих случаях, предложений, содержащихся в докладе РГОС 2021 года и резюме, подготовленном Председателем[38].

36. 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[39]:

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 перечень тем, предложенных государствами для дальнейшего обсуждения и касающихся международного права, включает следующие темы: как нормы международного права, в частности Устав Организации Объединенных Наций, применяются 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 применяются нормы международного права; и предложения, содержащиеся в докладе РГОС 2021 года и резюме, подготовленном Председателем, 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»[40];

[38] Второй ежегодный доклад о проделанной работе, п. 28.
[39] Второй ежегодный доклад о проделанной работе, пп. 29 a) и b).
[40] Доклад РГОС 2021 года (A/75/816), приложение I, п. 80.

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 признала необходимость дальнейшего изучения вопроса о том, как и когда эти принципы применяются к использованию ИКТ государствами, и подчеркнула, что напоминание об этих принципах ни в коем случае не узаконивает и не поощряет конфликты»[41].

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

a) подтвердили принципы государственного суверенитета и суверенного равенства[42]. Кроме того, государства подтвердили, что суверенитет государств и международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над ИКТ-инфраструктурой, расположенной на их территории. К деятельности государств в сфере использования ИКТ применимы существующие обязательства по международному праву. Государства осуществляют юрисдикцию в отношении ИКТ-инфраструктуры на своей территории, в частности, принимая политические и законодательные меры и создавая необходимые механизмы для защиты ИКТ-инфраструктуры на своей территории от связанных с ИКТ угроз[43];

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»[44]; 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 мирными средствами по своему выбору»[45];

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[46];

---

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

[42] Второй ежегодный доклад о проделанной работе, п. 30 a).

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

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

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

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

e) кроме того, они подчеркнули, что поведение с использованием ИКТ, которое не является нарушением запрета на угрозу силой или ее применение, может, в зависимости от обстоятельств, противоречить другим принципам международного права, таким как государственный суверенитет или запрет на вмешательство во внутренние или внешние дела государств.

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

a) государства отметили дискуссии по вопросам международного права, состоявшиеся на шестой, седьмой и восьмой сессиях, а также на межсессионных совещаниях РГОС, и приветствовали активное участие в этих дискуссиях все большего числа государств. Государства отметили, что за время работы РГОС такие дискуссии по вопросам международного права значительно углубились, и предложили и впредь привлекать экспертов, например из Комиссии международного права или научных кругов, для проведения брифингов в ходе таких дискуссий при должном учете справедливого географического представительства и национальных контекстов;

b) государства подтвердили, что нормы международного права, в частности Устав Организации Объединенных Наций, применимы и существенно важны для поддержания мира и стабильности и содействия созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды[47], и предложили более подробно обсудить в рамках РГОС вопрос о том, как нормы международного права применяется к использованию ИКТ с учетом специфики среды ИКТ;

c) государства отметили также, что обмен национальными мнениями и информацией о позициях в отношении международного права мог бы способствовать формированию общего понимания в вопросе о том, как нормы международного права применяются к использованию ИКТ, и настоятельно призвали продолжать добровольный обмен такими национальными мнениями и информацией о позициях в отношении международного права, который может включать национальные заявления и сведения о практике государств в отношении того, как нормы международного права применяются к использованию ИКТ. Кроме того, в выработке такого общего понимания государствам могут помочь соответствующие исследования и мнения экспертов в области международного права[48];

d) признавая существующие инициативы по наращиванию потенциала в области международного права, государства вновь подчеркнули настоятельную необходимость продолжения такой работы по наращиванию потенциала, в том числе с целью обеспечения всем государствам возможностей на равных участвовать в выработке общего понимания относительно того, как нормы международного права применяются к использованию ИКТ. Такая работа по наращиванию потенциала может включать проведение практикумов, учебных курсов, конференций и обменов передовым опытом на международном, межрегиональном, региональном и субрегиональном уровнях, а также, сообразно обстоятельствам, использование опыта соответствующих региональных организаций и должна осуществляться в соответствии с принципами наращивания потенциала, изложенными в пункте 56 доклада РГОС 2021 года[49];

[47] Доклад РГОС 2021 года, п. 34.

[48] Второй ежегодный доклад о проделанной работе, п. 31 b).

[49] Второй ежегодный доклад о проделанной работе, п. 31 c).

e) 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 норм действующего международного права к использованию ИКТ, и дальнейшего рассмотрения вопроса о разработке дополнительных юридически обязывающих обязательств[50].

Рекомендуемые дальнейшие действия

39. **Государствам рекомендуется и далее участвовать в проводимых в рамках РГОС целенаправленных обсуждениях вопросов применения норм международного права к использованию ИКТ, опираясь, в соответствующих случаях, на темы из неисчерпывающего перечня, приведенные в пунктах 36–38 выше, а также на предложения по теме международного права, содержащиеся в докладе РГОС 2021 года и резюме, подготовленном Председателем.**

40. **В развитие обсуждений, состоявшихся на шестой, седьмой и восьмой сессиях РГОС, государствам предлагается продолжать добровольный обмен национальными мнениями и информацией о позициях, который может включать национальные заявления и сведения о практике государств в отношении того, как нормы международного права применяются к использованию ИКТ. Секретариату Организации Объединенных Наций предлагается публиковать эти мнения на веб-сайте РГОС, чтобы все государства могли с ними ознакомиться и чтобы РГОС могла продолжить их обсуждение на ее предстоящих основных сессиях.**

41. **Государствам, которые имеют такую возможность, рекомендуется 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 относительно того, как нормы международного права применяются 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.**

E. Меры укрепления доверия

42. В ходе шестой, седьмой и восьмой сессий, а также специальных межсессионных совещаний РГОС государства продолжили обсуждение вопроса о мерах укрепления доверия. Государства подтвердили значение кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ и выступили с конкретными, ориентированными на практические действия предложениями в отношении мер укрепления доверия. Ниже приводится неисчерпывающий перечень предложений, которые были в той или иной степени поддержаны государствами и которые могут быть доработаны и дополнены на предстоящих сессиях РГОС:

a) государства вновь подчеркнули, что меры укрепления доверия имеют существенно важное значение для укрепления взаимного доверия и повышения

[50] Второй ежегодный доклад о проделанной работе, п. 32.

степени предсказуемости в отношениях между государствами, а также для снижения напряженности и уменьшения риска просчетов и недоразумений. Государства подчеркнули также взаимосвязь между мерами укрепления доверия и другими аспектами рамок ответственного поведения государств в области использования ИКТ;

b) государства приветствовали открытие 9 мая 2024 года Глобального реестра контактных пунктов и проведение в тот же день первого совещания представителей контактных пунктов. Кроме того, государства выразили признательность Секретариату за первое пинг-тестирование Глобального реестра контактных пунктов, проведенное 10 июня 2024 года. Государства напомнили о целях и принципах Глобального реестра контактных пунктов, изложенных в приложении A ко второму ежегодному докладу о проделанной работе[51], отметив также, что Глобальный реестр может способствовать продвижению мер укрепления доверия в целом. В этой связи государства подчеркнули необходимость продолжения работы по дальнейшему развитию и введению в действие Глобального реестра на предстоящих сессиях РГОС и впоследствии под эгидой будущего постоянного механизма;

c) государства подчеркнули, что для развития Глобального реестра контактных пунктов можно было бы использовать поэтапный подход, основанный на опыте его практического использования. В качестве задачи первостепенной важности всем государствам — членам Организации Объединенных Наций, которые еще не сделали этого, было рекомендовано как можно скорее утвердить национальные контактные пункты. Такие меры, как повышение степени осведомленности о важности контактных пунктов для безопасности ИКТ в национальном политическом контексте и целенаправленное наращивание потенциала, могут способствовать тому, чтобы как можно больше государств назначали представителей национальных контактных пунктов для включения в Глобальный реестр. РГОС призвала государства, которые в состоянии сделать это, оказать поддержку представителям национальных контактных пунктов из развивающихся стран для участия в очных заседаниях представителей национальных контактных пунктов в рамках РГОС;

d) государства предложили также разработать в целях оптимизации связи между государствами через Глобальный реестр контактных пунктов стандартные шаблоны для повышения ясности и оперативности связи между государствами. В то же время государства отметили также, что такие шаблоны должны быть гибкими и добровольными, чтобы не создавать излишних трудностей при использовании Глобального реестра, особенно в экстренных ситуациях;

e) в дополнение к уже рекомендованным мерам укрепления доверия, которые были изложены в предыдущих докладах Организации Объединенных Наций, в том числе в приложении B ко второму ежегодному докладу о проделанной работе, озаглавленном «Первоначальный перечень добровольных глобальных мер укрепления доверия», государства внесли предложения по дополнительным глобальным мерам укрепления доверия, которые содержатся в приложении B к настоящему докладу;

f) государства высказали мнение о том, что обмен национальными мнениями относительно технических терминов и терминологии в сфере ИКТ мог бы способствовать повышению степени транспарентности и взаимопонимания

[51] A/78/265.

между государствами. Государства могли бы продолжать обмениваться мнениями о таких технических терминах и терминологии;

g) было высказано предложение о том, что аспекты мер укрепления доверия могут, сообразно обстоятельствам, и далее предусматривать взаимодействие с другими заинтересованными сторонами и субъектами, включая представителей деловых кругов, неправительственных организаций и научного сообщества[52];

h) 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[53]. Кроме того, государства подчеркнули, что РГОС может стать платформой для инновационного применения мер укрепления доверия.

Рекомендуемые дальнейшие действия

43. **Государствам рекомендуется продолжить в рамках РГОС обмен мнениями по вопросу о разработке и имплементации мер укрепления доверия, в том числе о возможной разработке дополнительных мер укрепления доверия с учетом пунктов 42 a)–h) выше.**

44. **Государствам рекомендуется продолжить работу по дальнейшему развитию и введению в действие Глобального реестра на предстоящих сессиях РГОС и впоследствии под эгидой будущего постоянного механизма. В качестве задачи первостепенной важности всем государствам — членам Организации Объединенных Наций, которые еще не сделали этого, рекомендуется как можно скорее утвердить национальные контактные пункты для включения в Глобальный реестр контактных пунктов. Кроме того, государствам, которые в состоянии делать это, предлагается оказывать поддержку представителям национальных контактных пунктов из развивающихся стран для участия в очных заседаниях представителей национальных контактных пунктов в рамках РГОС.**

45. **Государствам предлагается активно участвовать в проводимых раз в полгода пинг-тестах для контактных пунктов, как это предусмотрено в приложении A ко второму ежегодному докладу о проделанной работе[54].**

46. **В соответствии с приложением A ко второму ежегодному докладу о проделанной работе[55] Председателю РГОС рекомендуется организовать имитационное испытание в смешанном формате в партнерстве с заинтересованными государствами и структурами Организации Объединенных Наций и при поддержке Секретариата Организации Объединенных Наций.**

47. **Государствам рекомендуется оптимизировать коммуникацию через Глобальный реестр контактных пунктов, в том числе путем разработки стандартизированных шаблонов для использования государствами по их усмотрению. В этой связи Секретариату Организации Объединенных Наций предлагается, опираясь на предложения государств, а также, в случае необходимости, на опыт региональных организаций, разработать к апрелю 2025 года пример такого шаблона с целью выработки консенсусной рекомендации.**

---

[52] Второй ежегодный доклад о проделанной работе, п. 31 f).

[53] Второй ежегодный доклад о проделанной работе, п. 31 g).

[54] Пункт 8.

[55] Пункт 13 e).

48. **Ссылаясь на перечень глобальных мер укрепления доверия, содержащийся в приложении B ко второму ежегодному докладу о проделанной работе[56], государства рекомендуют использовать меры укрепления доверия, изложенные в приложении B к настоящему докладу, в качестве дополнительных добровольных глобальных мер укрепления доверия, признавая, что государства могут осуществлять меры укрепления доверия в соответствии с их различными национальными задачами первостепенной важности и возможностями. Председателю РГОС предлагается содействовать продолжению обсуждения путей 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.**

49. **Государствам предлагается на добровольной основе продолжать обмениваться национальными мнениями относительно технических терминов и терминологии в сфере ИКТ для повышения степени транспарентности и взаимопонимания в отношениях между государствами[57].**

F. Наращивание потенциала

50. В ходе шестой, седьмой и восьмой сессий, а также специальных межсессионных совещаний РГОС государства продолжили обсуждение вопроса о наращивании потенциала ИКТ в контексте международной безопасности. В ходе этих сессий государства поделились национальным опытом в сфере международного сотрудничества и наращивания потенциала, а также текущими двусторонними, региональными и глобальными инициативами по наращиванию потенциала ИКТ в контексте международной безопасности. Государства подтвердили значение кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ и выступили с конкретными, ориентированными на практические действия предложениями в отношении наращивания потенциала ИКТ в контексте международной безопасности. Ниже приводится неисчерпывающий перечень предложений, которые были в той или иной степени поддержаны государствами и которые могут быть доработаны и дополнены на предстоящих сессиях РГОС:

a) государства напомнили и подтвердили принципы наращивания потенциала в области безопасности ИКТ, принятые в докладе РГОС 2021 года, вновь подчеркнули необходимость дальнейших усилий по включению этих принципов в соответствующие программы наращивания потенциала. 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[58];

b) подчеркнув, что универсального решения проблемы наращивания потенциала не существует, государства предложили, чтобы усилия по наращиванию потенциала с учетом потребностей государства-получателя, которые могут включать передачу знаний, навыков и технологий на взаимно согласованных условиях, были подкреплены оценкой государством своего собственного текущего состояния безопасности ИКТ на национальном уровне. Такие меры

[56] A/78/265.
[57] Второй ежегодный доклад о проделанной работе, п. 42.
[58] Второй ежегодный доклад о проделанной работе, п. 43 a).

позволят выявить пробелы, а также помогут установить четкие, достижимые цели в плане обеспечения соблюдения и использования кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ. Кроме того, государства подчеркнули необходимость расширения доступности программ наращивания потенциала и обеспечения лидерства в сфере безопасности ИКТ, предназначенных для старших должностных лиц и лиц, принимающих решения на национальном уровне. В этой связи государства вновь подчеркнули ценность сотрудничества Юг — Юг, трехстороннего и субрегионального и регионального сотрудничества, которое не заменяет собой, а дополняет сотрудничество Север — Юг;

c) государства продолжили обсуждение инициативы по созданию глобального портала сотрудничества в области кибербезопасности и предложили сделать его практичной и нейтральной, модульной платформой «единого окна» для государств, созданной по инициативе государств-участников и разработанной под эгидой Организации Объединенных Наций. Предполагается, что этот портал мог бы стать платформой для координации действий государств по вопросам обеспечения безопасности ИКТ и обеспечивать достаточную гибкость с учетом потребностей государств в отношении рамок ответственного поведения при использовании ИКТ по решению государств. Кроме того, этот портал можно было бы согласовать с существующими и смежными онлайн-порталами. Впоследствии этот портал будет поддерживать и облегчать работу будущего постоянного механизма и способствовать обеспечению взаимодополняемости и избежанию дублирования с существующими инициативами;

d) кроме того, было внесено предложение о разработке каталога возможностей по наращиванию потенциала в области обеспечения безопасности ИКТ с учетом потребностей, чтобы помочь государствам в определении потребностей в наращивании потенциала и предоставлять доступ к информации о способах подачи заявок на участие в программах по наращиванию потенциала. Такой каталог можно было бы также согласовать с глобальным порталом сотрудничества в области кибербезопасности, если оба этих портала будут созданы по инициативе государств;

e) государства приветствовали проведение 10 мая 2024 года в Нью-Йорке глобального круглого стола высокого уровня по вопросам наращивания потенциала ИКТ в контексте международной безопасности. Этот круглый стол позволил внести дополнительный вклад в дискуссии РГОС, поскольку благодаря ему высокопоставленные государственные должностные лица смогли получить более глубокое представление о безотлагательности задачи наращивания потенциала ИКТ, в то время как дискуссионные форумы с участием специалистов-практиков по наращиванию потенциала способствовали обмену информацией и передовым опытом по практическим вопросам деятельности по наращиванию потенциала. Государства предложили и в будущем регулярно созывать подобные круглые столы по вопросам наращивания потенциала ИКТ в контексте международной безопасности;

f) государства отметили проведенное Секретариатом Организации Объединенных Наций мероприятие по картированию[59] с целью изучения ситуации с программами и инициативами по наращиванию потенциала в рамках Организации Объединенных Наций и за ее пределами, а также на глобальном и региональном уровнях. В этой связи государства подчеркнули, что необходимо обеспечить дальнейшую координацию усилий по наращиванию потенциала в области безопасности ИКТ и что Организация Объединенных Наций могла бы играть

[59] A/AC.292/2024/2.

важную роль в таких усилиях. Государства отметили, что эти усилия должны исключать дублирование с аналогичными инициативами. В то же время, с учетом существующих способов финансирования деятельности по наращиванию потенциала ИКТ в контексте международной безопасности, государствам было предложено продолжать рассматривать дополнительные способы финансирования под эгидой будущего постоянного механизма по обеспечению безопасности ИКТ в контексте международной безопасности, в том числе путем координации с существующими программами развития и соответствующими механизмами финансирования;

g) государства признали, что сама РГОС могла бы стать инклюзивной 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 и потенциала в сфере применения рамок ответственного поведения государства в области использования ИКТ. Государства подчеркнули, что РГОС могла бы также использоваться в качестве платформы для обмена передовым опытом по наращиванию потенциала по обеспечению безопасности ИКТ, а также для продолжения работы по созданию механизмов сотрудничества для устранения угроз, возникающих при использовании ИКТ. Было отмечено, что такая работа должна дополнять деятельность, уже осуществляемую в других структурах системы Организации Объединенных Наций;

h) государства, в том числе через РГОС, могут продолжать укреплять координацию и сотрудничество между государствами и другими заинтересованными сторонами и субъектами, включая представителей деловых кругов, неправительственных организаций и научного сообщества. Государства подчеркнули также, что к работе РГОС можно было бы привлечь и молодежь. Государства отметили, что другие заинтересованные стороны и субъекты, включая деловые круги, неправительственные организации и научное сообщество, уже играют важную роль в рамках партнерства с государствами, в том числе для целей подготовки кадров и проведения исследований. Другие заинтересованные стороны и субъекты, включая деловые круги, неправительственные организации и научное сообщество, могли бы использовать результаты работы РГОС по наращиванию потенциала, а также высказать свои мнения об этих усилиях;

i) государства подтвердили важность вопроса о наращивании потенциала не только в качестве сквозного вопроса в работе РГОС, но и в плане повышения уровня осведомленности и содействия общему пониманию рамок ответственного поведения государств в области использования ИКТ.

Рекомендуемые дальнейшие действия

51. **Государствам рекомендуется продолжить обмен мнениями в рамках РГОС по вопросу о наращивании потенциала ИКТ в контексте международной безопасности, в том числе по пунктам 50 a)–i) выше.**

52. **Секретариату Организации Объединенных Наций предлагается подготовить для рассмотрения РГОС первоначальный доклад с изложением предложения по разработке и введению в действие специального Глобального портала сотрудничества и наращивания потенциала в области безопасности ИКТ, принимая во внимание смежные инициативы, с целью оптимизации синергетического эффекта и избежания дублирования. Государствам предлагается представить свои мнения относительно создания портала, который стал бы: a) практичной и нейтральной, модульной платформой «единого окна» для государств, созданной по инициативе государств-**

участников и разработанной под эгидой Организации Объединенных Наций; b) архивом для хранения мнений и рабочих документов, представленных государствами по темам, касающимся обеспечения безопасности при использовании ИКТ, и местом публикации календаря мероприятий, связанных с вопросами обеспечения безопасности при использовании ИКТ; c) местом публикации основанного на потребностях каталога возможностей по наращиванию потенциала в области безопасности ИКТ с использованием, сообразно обстоятельствам, результатов работы, проделанной на существующих порталах, в целях оказания государствам помощи в определении потребностей в наращивании потенциала и в доступе к информации об имеющихся ресурсах для удовлетворения выявленных потребностей. Секретариату Организации Объединенных Наций предлагается подготовить первоначальный доклад на основе мнений государств и пунктов a)-c) выше, а также вовремя представить его для рассмотрения на десятой основной сессии РГОС в марте 2025 года. Впоследствии этот портал будет поддерживать и облегчать работу будущего постоянного механизма.

53. **В целях обеспечения постоянного внимания к насущной проблеме наращивания потенциала в области безопасности ИКТ государствам рекомендуется регулярно созывать под эгидой будущего постоянного механизма глобальные круглые столы высокого уровня по вопросам наращивания потенциала в области безопасности ИКТ, что позволит проводить стратегические, а также ориентированные на конкретные действия обсуждения по вопросу наращивания потенциала в контексте безопасности ИКТ. В таких круглых столах могли бы принимать участие специалисты-практики в области наращивания потенциала, представители заинтересованных государств и других заинтересованных сторон и субъектов, включая представителей деловых кругов, неправительственных организаций и научного сообщества, при должном учете справедливой географической представленности. Государствам, которые в состоянии делать это, рекомендуется оказывать поддержку представителям и экспертам из развивающихся стран для участия в таких круглых столах.**

54. **Государствам рекомендуется продолжить изучение вопроса о создании фонда добровольных взносов Организации Объединенных Наций, максимально используя существующие инициативы, для поддержки деятельности по наращиванию потенциала государств в области безопасности при использовании ИКТ. Этот фонд, в частности, способствовал бы участию национальных представителей и экспертов, особенно из развивающихся стран, в соответствующих совещаниях в рамках будущего постоянного механизма по вопросам безопасности ИКТ в контексте международной безопасности, а также достижению других целей, определенных государствами. Секретариату Организации Объединенных Наций предлагается подготовить для рассмотрения РГОС первоначальный доклад с изложением предложения по разработке и введению в действие этого фонда добровольных взносов для рассмотрения государствами к моменту рассмотрения на десятой основной сессии РГОС в марте 2025 года на предмет выработки к июлю 2025 года консенсусной рекомендации по этим деталям для введения фонда в действие под эгидой будущего постоянного механизма. При подготовке этого предложения Секретариату Организации Объединенных Наций предлагается рассмотреть, в частности, вопросы, касающиеся определения надлежащего управляющего для этого фонда; финансовых и административных требований; критериев для отбора потенциальных бенефициаров и предоставления им доступа к средствам фонда; мониторинга и оценки; и способов учета принципов наращивания потенциала в области безопасности**

ИКТ в процессе создания фонда. Секретариату Организации Объединенных Наций предлагается также стремиться обеспечивать взаимодополняемость и избегать дублирования с существующими инициативами, а также исходить из того, что этот фонд может получать финансовые ресурсы из государственных, частных и благотворительных источников.

55. **Государствам, которые имеют такую возможность, рекомендуется продолжать поддерживать программы по наращиванию потенциала, в том числе в сотрудничестве, сообразно обстоятельствам, с региональными и субрегиональными организациями и другими заинтересованными сторонами и субъектами, включая представителей деловых кругов, неправительственных организаций и научного сообщества.**

G. Регулярный институциональный диалог

56. В ходе шестой, седьмой и восьмой сессий, а также специальных межсессионных совещаний РГОС государства продолжили обсуждение вопроса о регулярном институциональном диалоге в соответствии с рекомендациями, сформулированными во втором ежегодном докладе о проделанной работе[60]. Государства подтвердили значение кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ и выступили с конкретными, ориентированными на практические действия предложениями в отношении регулярного институционального диалога:

a) в развитие целей, которые были установлены в соответствующих резолюциях Генеральной Ассамблеи, включая, в частности, резолюции 78/16 и 78/237, касающиеся обсуждения вопроса о регулярном институциональном диалоге в рамках РГОС, и в соответствии с рекомендациями, содержащимися в докладе РГОС 2021 года[61] и в первом[62] и втором[63] ежегодных докладах РГОС о проделанной работе, государства провели углубленное обсуждение возможных элементов будущего постоянного механизма;

b) государства выразили готовность продолжить обсуждения с целью достижения консенсуса по вопросу создания одновекторного будущего постоянного механизма. В этой связи государства рассмотрели подготовленный Председателем документ под названием «Элементы открытого прикладного постоянного механизма по безопасности ИКТ в контексте международной безопасности», в котором содержатся элементы, касающиеся руководящих принципов; функций и объема работы; структуры; порядка функционирования и процесса принятия решений в рамках будущего постоянного механизма.

57. Государства выступили с предложением о том, чтобы будущий постоянный механизм способствовал дальнейшему внедрению и последующему развитию всех существующих инициатив, выдвинутых под эгидой РГОС 2021–2025 годов, и/или других начатых ранее процессов, включая, в частности, процесс создания Глобального реестра контактных пунктов и проведения глобального круглого стола по вопросам наращивания потенциала в сфере безопасности ИКТ.

[60] Пункты 54–59.

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

[62] Первый ежегодный доклад о проделанной работе, раздел «Регулярный институциональный диалог», подраздел «Рекомендуемые дальнейшие действия», пункт 2.

[63] Второй ежегодный доклад о проделанной работе, пп. 54–59.

Рекомендуемые дальнейшие действия

58. **Государства рекомендуют создать будущий постоянный механизм на основе консенсусных элементов, содержащихся в документе под названием «Элементы открытого прикладного постоянного механизма по безопасности ИКТ в контексте международной безопасности», который приводится в приложении C к настоящему докладу, с тем чтобы обеспечить плавный переход от РГОС к будущему постоянному механизму.**

59. **Государствам рекомендуется продолжить обсуждения в рамках нынешней РГОС и представить в заключительном докладе РГОС, который будет принят в июле 2025 года, рекомендации по следующим вопросам: a) условия участия в будущем постоянном механизме других заинтересованных сторон и субъектов, включая представителей деловых кругов, неправительственных организаций и научного сообщества; b) специальные тематические группы для рассмотрения в рамках будущего постоянного механизма; c) другие элементы, которые могут потребоваться.**

60. **Государства рекомендовали, чтобы будущий постоянный механизм способствовал дальнейшему внедрению и последующему развитию всех существующих инициатив, выдвинутых под эгидой РГОС 2021-2025 годов, и/или других начатых ранее процессов, включая, в частности, процесс создания Глобального реестра контактных пунктов и проведения глобального круглого стола по вопросам наращивания потенциала в сфере безопасности ИКТ.**

Приложение A

Добровольный контрольный перечень практических действий по реализации добровольных, не имеющих обязательной силы норм ответственного поведения государств при использовании ИКТ

1. Во втором Ежегодном докладе о проделанной РГОС работе государства предложили следующее рекомендуемое дальнейшее действие: «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[1]».

2. Предполагается, что этот контрольный перечень станет добровольным инструментом наращивания потенциала, который государства могут пожелать использовать в рамках своих усилий по реализации добровольных, не имеющих обязательной силы норм ответственного поведения государств в сфере использования ИКТ. Кроме того, государства признали, что контрольный перечень может стать полезным инструментом наращивания потенциала для определения базовых возможностей, необходимых государствам для повышения степени устойчивости в плане обеспечения безопасности ИКТ. В этой связи указанный контрольный перечень может a) служить отправной точкой для поддержки имплементационных усилий государств, b) стать полезным инструментом оценки и подспорьем в определении первоочередных задач целенаправленных усилий по наращиванию потенциала и c) использоваться в качестве общего ориентира для поддержки обмена передовым опытом в конкретных областях безопасности ИКТ. Он является «живым документом», который можно было бы периодически обновлять.

3. В целом, реализация добровольных, не имеющих обязательной силы норм может потребовать от государств принятия некоторых общих мер практического характера.

На национальном уровне такие меры могли бы включать:

a) создание групп реагирования на компьютерные инциденты (CERTs) или групп реагирования на инциденты в сфере компьютерной безопасности (CSIRTs) и других национальных координационных структур и механизмов;

b) разработку национальных законов и политики в области ИКТ, включая национальную стратегию в области ИКТ.

На международном уровне действия государств по поддержке реализации норм могли бы включать:

a) участие в осуществлении инклюзивных международных, межрегиональных, региональных и субрегиональных процессов в сфере ИКТ, связанных с безопасностью ИКТ;

b) участие в обмене информацией и передовым опытом по различным аспектам безопасности ИКТ;

[1] Второй ежегодный доклад РГОС о проделанной работе (A/78/265), п. 26.

c) внесение предложений относительно оказания помощи в связи с инцидентами, связанными с ИКТ, и запрашивание такой помощи с использованием таких каналов, как Глобальный реестр контактных лиц.

4. Наращивание потенциала является ключевым фактором для того, чтобы все государства могли осуществлять эти практические действия, и поэтому оно является одним из центральных компонентов обеспечения реализации норм на глобальном уровне. В то же время государства признают, что универсального решения в отношении реализации норм не существует, поэтому при использовании предлагаемого контрольного перечня для реализации норм следует учитывать различия в техническом потенциале между государствами, различные национальные системы и региональную специфику.

5. Этот контрольный перечень практических действий не является исчерпывающим по своему характеру. Любое использование государствами этого контрольного перечня является полностью добровольным. В процессе разработки и использования этого контрольного перечня государства напоминают и подтверждают предыдущие договоренности, которые являются элементами, закрепляющими кумулятивные и эволюционирующие рамки ответственного поведения государств в области использования ИКТ[2].

[2] Государства подтвердили консенсусные первый и второй ежегодные доклады нынешней РГОС о проделанной работе (A/77/275 и A/78/265), консенсусный доклад РГОС 2021 года о достижениях в сфере ИКТ в контексте международной безопасности (A/75/816) и консенсусные доклады ГПЭ 2010, 2013, 2015 и 2021 годов (A/65/201, A/68/98, A/70/174 и A/76/135). См. второй ежегодный доклад о проделанной работе (A/78/265), п. 3.

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

Добровольные практические действия по реализации этой нормы

Действия на национальном уровне

☐ 1. Принять или укрепить национальную политику, законодательство и соответствующие процессы обзора для поддержки или облегчения международного сотрудничества[3].

☐ 2. Создать или укрепить национальные структуры и механизмы[4] для выявления инцидентов в сфере ИКТ, защиты от них, реагирования на них и восстановления после них.

☐ 3. Создать или укрепить общегосударственные механизмы и политику сотрудничества и партнерства для поддержки или облегчения международного сотрудничества[5].

☐ 4. Создать или укрепить механизмы сотрудничества и диалога с частным сектором, научным сообществом, гражданским обществом и техническим сообществом[6].

☐ 5. Провести добровольное исследование национальных усилий и обмен национальным опытом по реализации норм[7]. Это можно было бы сделать в рамках доклада Генерального секретаря о достижениях в сфере ИКТ в контексте международной безопасности, а также Обзора хода реализации на национальном уровне[8].

---

[3] Доклад ГПЭ 2021 года (A/76/135), пункт 21; принятая на основе консенсуса резолюция 76/19 Генеральной Ассамблеи.

[4] A/76/135, пункт 21. Дополнительное примечание: такие структуры и механизмы могут включать: национальный центр или ответственное агентство или головное ведомство по вопросам безопасности ИКТ; и группы реагирования на компьютерные инциденты (CERTs) или группы реагирования на инциденты в сфере компьютерной безопасности (CSIRTs).

[5] A/76/135, п. 21.

[6] A/76/135, п. 21.

[7] A/76/135, п. 21.

[8] Первый ежегодный доклад РГОС о проделанной работе (A/77/275), раздел «Рекомендуемые дальнейшие действия», касающийся правил, норм и принципов ответственного поведения государств, пункт 3.

Действия, требующие международного сотрудничества

☐ 6. Участвовать, где это уместно, в работе региональных и субрегиональных организаций, которые способствуют сотрудничеству между государствами в сфере использования ИКТ в контексте международной безопасности[9].

Предложение о дополнительных действиях

- Рассмотреть возможность участия в работе таких инклюзивных и транспарентных механизмов, как Глобальный реестр контактных пунктов, для развития сотрудничества и обмена информацией.

[9] Признав, что не все государства являются членами региональных организаций и не все региональные организации делают упор на вопросы безопасности в области использования ИКТ, РГОС отметила, что прилагаемые на региональном уровне усилия служат дополнением к ее работе (первый и второй ежегодные доклады РГОС о проделанной работе (A/77/275, пункт 5 и A/78/265, пункт 7).

Норма b)
Государства должны изучить в случае инцидентов в сфере ИКТ всю соответствующую информацию, в том числе более широкий контекст события, проблемы установления ответственности в ИКТ-среде, а также характер и масштабы ответственности.

Добровольные практические действия по реализации этой нормы

Действия на национальном уровне

☐ 1. Создать или укрепить соответствующие национальные структуры, политику, процессы, законодательную базу и координационные механизмы, связанные с ИКТ, для оценки степени серьезности и вероятности повторения инцидентов в сфере ИКТ. Это может включать создание партнерств и использование других форм взаимодействия с соответствующими заинтересованными субъектами[10].

☐ 2. В случае возникновения инцидента в сфере ИКТ при его оценке необходимо учитывать все аспекты[11]. Такие подтвержденные фактами оценки могут включать:

- технические характеристики инцидента;
- его охват, масштабы и последствия;
- более широкий контекст, в том числе воздействие этого инцидента на международный мир и безопасность; и
- результаты консультаций между имеющими к нему отношение государствами[12].

☐ 3. Определить процедуры принятия мер реагирования на злонамеренную деятельность с использованием ИКТ, приписываемую другому государству, в соответствии с обязательствами государства по Уставу Организации Объединенных Наций и другим нормам международного права, в том числе обязательствами, касающимися мирного урегулирования споров и международно-противоправных деяний[13].

Действия, требующие международного сотрудничества

☐ 4. Обеспечить сотрудничество между национальными группами реагирования на компьютерные инциденты (CERTs) и группами реагирования на инциденты в сфере компьютерной безопасности (CSIRTs), государственными органами, занимающимися вопросами ИКТ, и дипломатическим сообществом в целях укрепления способности государств выявлять и расследовать злонамеренные инциденты в сфере использования ИКТ, а также обосновывать свои озабоченности и соответствующие выводы перед вынесением заключения об инциденте[14].

---

[10] A/76/135, пункт 26.

[11] Установление ответственности, которое является комплексной задачей, и определение источника инцидента в сфере ИКТ, которое требует рассмотрения широкого круга факторов. Необходимо проявлять осторожность, в том числе изучить вопрос о том, как применяются нормы международного права, во избежание недопонимания и эскалации напряженности в отношениях между государствами (A/76/135, пункт 22).

[12] A/76/135, п. 24.

[13] A/76/135, п. 25.

[14] A/76/135, п. 27.

☐ 5. Использовать многосторонние, региональные и двусторонние платформы, а также платформы с участием многих заинтересованных сторон для обмена практическим опытом и информацией о национальных подходах к установлению ответственности, в том числе о том, как государства могут различать виды установления ответственности, и об угрозах и инцидентах, связанных с ИКТ[15].

☐ 6. Всем сторонам, вовлеченным в инцидент в сфере ИКТ, рекомендуется проводить консультации друг с другом по линии соответствующих компетентных органов[16].

☐ 7. Установить процедуры для мирного урегулирования споров[17] в связи с инцидентами в сфере ИКТ посредством переговоров, расследования, посредничества, примирения, арбитража, судебного разбирательства, обращения к региональным органам или механизмам или иными мирными средствами по своему выбору[18].

Предложение о дополнительных действиях

- Рассмотреть возможность использования, сообразно обстоятельствам, таких многосторонних каналов связи на дипломатическом и техническом уровнях, таких как Глобальный реестр контактных пунктов, для обмена информацией и проведения консультаций между государствами в случае инцидента в сфере ИКТ.

[15] A/76/135, п. 28.
[16] A/76/135, п. 23.
[17] A/76/135, п. 25.
[18] Устав Организации Объединенных Наций, пункт 1 статьи 33.

Норма c)
Государствам не следует заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ.

Добровольные практические действия по реализации этой нормы

Действия на национальном уровне

☐ 1. Если международно-противоправное деяние происходит в пределах территории государства, то это государство будет предпринимать разумные и посильные действия, с тем чтобы положить конец деятельности, происходящей с их территории, используя соразмерные, надлежащие и эффективные методы таким образом, чтобы это соответствовало нормам международного права и внутреннему законодательству. Не предполагается, что государство может или должно отслеживать всю деятельность с использованием ИКТ на своей территории[19].

☐ 2. Создать и использовать структуры и механизмы для формулирования предложений об оказании помощи и реагирования на запросы об оказании помощи в случае инцидента в сфере ИКТ[20].

Действия, требующие международного сотрудничества

☐ 3. В случае инцидента в сфере ИКТ можно предпринять следующие шаги:

- Пострадавшее государство должно уведомить государство, с территории которого исходит деятельность[21].
- Уведомляемое государство должно подтвердить получение уведомления для содействия сотрудничеству и прояснению вопроса. Подтверждение получения такого уведомления не означает согласия с содержащейся в нем информацией[22].
- Уведомляемое государство должно приложить все разумные усилия для оказания помощи в установлении факта совершения международно-противоправного деяния[23].

---

[19] A/76/135, п. 30 a).

[20] Государство, которое знает о совершении международно-противоправных деяний с применением ИКТ, расположенных на его территории, но не располагает возможностями для решения этой проблемы, может рассмотреть возможность обращения за помощью к другим государствам или представителям частного сектора в соответствии с положениями международного права и внутреннего законодательства. При оказании помощи государствам следует действовать добросовестно, в соответствии с нормами международного права, и не использовать такую возможность для совершения злонамеренных действий против государства, обращающегося за помощью, или против третьего государства (доклад ГПЭ 2021 года (A/76/135), п. 30 b)).

[21] A/76/135, п. 30 c).

[22] A/76/135, п. 30 c).

[23] A/76/135, п. 30 c). Сам по себе инцидент в сфере использования ИКТ, исходящий с территории третьего государства или осуществляемый с использованием его инфраструктуры, не подразумевает ответственности этого государства за данный инцидент. 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 (доклад ГПЭ 2021 года (A/76/135), п. 30 d), и второй ежегодный доклад о проделанной работе (A/78/265), приложение A, п. 10).

Предложение о дополнительных действиях

- Рассмотреть возможность использования, сообразно обстоятельствам, таких многосторонних каналов связи на дипломатическом и техническом уровнях, как Глобальный реестр контактных пунктов, для обмена информацией или реагирования на запросы об оказании помощи в случае инцидента в сфере ИКТ.

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

Добровольные практические действия по реализации этой нормы

Действия на национальном уровне

☐ 1. Разработать соответствующие протоколы и процедуры для сбора, обработки и хранения онлайн-доказательств, имеющих отношение к преступному и террористическому использованию ИКТ, в том числе для надлежащей работы с цепью обеспечения сохранности, в соответствии с обязательствами по международному праву[24].

☐ 2. Внедрить национальную политику, законодательство, структуры и механизмы, способствующие трансграничному сотрудничеству по техническим, правоохранительным, правовым и дипломатическим вопросам, имеющим отношение к борьбе с использованием ИКТ в преступных и террористических целях[25].

Действия, требующие международного сотрудничества

☐ 3. Укреплять и далее развивать механизмы, которые могут способствовать обмену информацией между соответствующими национальными, региональными и международными организациями для повышения степени осведомленности государств о безопасности в сфере использования ИКТ и уменьшения оперативного пространства для террористической и преступной деятельности онлайн[26].

☐ 4. Использовать существующие процессы, инициативы и правовые инструменты, а также рассмотреть возможность использования дополнительных процедур или каналов связи для содействия обмену информацией и оказанию помощи в борьбе с использованием ИКТ в преступных и террористических целях[27].

☐ 5. Своевременно оказывать помощь в проведении расследований, обеспечивая чтобы такие действия осуществлялись в соответствии с обязательствами государства по международному праву[28].

[24] A/76/135, п. 33.
[25] A/76/135, п. 32.
[26] A/76/135, п. 33.
[27] A/76/135, п. 35.
[28] A/76/135, п. 33.

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

Добровольные практические действия по реализации этой нормы

Действия на национальном уровне

☐ 1. Государства должны уважать и защищать права человека и основные свободы как в онлайн-, так и офлайн-среде в соответствии с взятыми на себя обязательствами[29].

☐ 2. Принять к сведению необходимость решения новых проблем и дилемм, возникших в связи с использованием государствами ИКТ, которые могут оказывать особенно негативное воздействие на осуществление и реализацию прав человека, в том числе согласно положениям новых резолюций Генеральной Ассамблеи[30].

☐ 3. Рассмотреть вопрос об инвестировании в разработку технических и правовых мер, призванных направлять развитие и использование ИКТ в более инклюзивном и доступном ключе без негативного воздействия на членов отдельных сообществ или групп, принимая во внимание последствия, которые новые и новейшие технологии могут иметь для прав человека и безопасности ИКТ[31].

☐ 4. Наладить взаимодействие с заинтересованными субъектами, которые по-разному содействуют защите и поощрению прав человека и основных свобод в онлайн- и офлайн-среде[32].

[29] A/76/135, п. 36.
[30] A/76/135, пп. 37 и 38.
[31] A/76/135, п. 40.
[32] A/76/135, п. 41.

Норма f)
Государства не должны заведомо осуществлять и поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит их обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения.

Добровольные практические действия по реализации этой нормы

Действия на национальном уровне

☐ 1. Определить, какие находящиеся в юрисдикции государства объекты инфраструктуры или сектора считаются критически важными в соответствии с национальными приоритетами и методами классификации объектов критически важной инфраструктуры[33].

☐ 2. Принять соответствующие директивные и законодательные меры на национальном уровне для обеспечения того, чтобы деятельность в области использования ИКТ, осуществляемая или поддерживаемая государством, которая может повлиять на критически важную инфраструктуру, используемую для оказания основных услуг населению другого государства, согласовывалась с этой нормой, использовалась в соответствии с его международно-правовыми обязательствами и подлежала всеобъемлющему обзору и надзору[34].

Действия, требующие международного сотрудничества

☐ 3. Сотрудничать с другими государствами в вопросах защиты критически важной инфраструктуры, обслуживающей несколько государств, как то техническая инфраструктура, необходимая для обеспечения общедоступности и надежности Интернета[35].

[33] A/76/135, п. 44.
[34] A/76/135, п. 46.
[35] A/76/135, п. 45.

Норма g)
Государства должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи.

Добровольные практические действия по реализации этой нормы

Действия на национальном уровне

☐ 1. Обеспечивать безопасность и защищенность ИКТ-продуктов на протяжении всего их жизненного цикла[36].

☐ 2. Классифицировать инциденты в сфере ИКТ с точки зрения их масштаба и серьезности[37].

Действия, требующие международного сотрудничества

☐ 3. Поощрять трансграничное сотрудничество с соответствующими владельцами и операторами объектов критически важной инфраструктуры в целях усиления мер безопасности в сфере использования ИКТ, принимаемых в отношении такой инфраструктуры, и укрепления существующих или разработки дополнительных процессов и процедур для выявления инцидентов в области использования ИКТ, затрагивающих такую инфраструктуру, и смягчения их последствий[38].

В рамках действий по реализации нормы g) государства могут также изучить возможность принятия во внимание перечня элементов, содержащегося в приложении к резолюции 58/199 Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур, а именно:

☐ 1. Наличие сетей для срочного предупреждения о факторах уязвимости, угрозах и инцидентах в сфере ИКТ.

☐ 2. Повышение степени информированности заинтересованных сторон, с тем чтобы они глубже понимали характер и масштабы своих важнейших информационных инфраструктур и ту роль, которую каждая из них должна играть в защите этих инфраструктур.

☐ 3. Анализ инфраструктур и выявление факторов, обусловливающих их взаимозависимость, для усиления защиты таких инфраструктур.

☐ 4. Содействие развитию партнерских отношений между заинтересованными сторонами, представляющими как государственный, так и частный секторы, для обмена информацией о важнейших инфраструктурах и ее анализа в целях предотвращения нанесения ущерба таким инфраструктурам или попыток нарушения их защиты, расследования таких случаев и принятия мер в связи с ними.

[36] A/76/135, п. 50.
[37] A/76/135, п. 50.
[38] A/76/135, п. 49.

☐ 5. Создание и обеспечение функционирования систем коммуникации в кризисной ситуации и проверка их функционирования для обеспечения их надежной и стабильной работы в чрезвычайных ситуациях.

☐ 6. Обеспечение того, чтобы процедуры предоставления доступа к данным учитывали необходимость защиты важнейших информационных инфраструктур.

☐ 7. Содействие отслеживанию попыток взлома защиты важнейших информационных инфраструктур и, в надлежащих случаях, предоставление информации о результатах такого отслеживания другим государствам.

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

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

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

☐ 11. Содействие национальным и международным научным исследованиям и опытно-конструкторским разработкам и поощрение применения технологий обеспечения защиты, отвечающих международным стандартам.

Предложение о дополнительных действиях

- Рассмотреть возможность определения структурных, технических, организационных, законодательных и нормативных мер и планов действий в чрезвычайных ситуациях, необходимых для защиты национальной критически важной инфраструктуры и восстановления работоспособности в случае возникновения инцидента.

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

Добровольные практические действия по реализации этой нормы

Действия на национальном уровне

☐ 1. Создать соответствующие национальные структуры и механизмы обнаружения и смягчения последствий инцидентов в сфере использования ИКТ, потенциально угрожающих международному миру и безопасности[39].

Действия, требующие международного сотрудничества

☐ 2. В случае необходимости, для смягчения последствий злонамеренной деятельности в сфере ИКТ, направленной против КВИ и КВИИ, запрашивать или предлагать помощь на двусторонней основе или в рамках региональных или международных соглашений с учетом должного уважения суверенитета[40].

☐ 3. Обращаться, сообразно обстоятельствам, к частному сектору за помощью в реагировании на просьбы об оказании помощи[41].

☐ 4. Принимать участие в работе совместных механизмов, определяющих средства и способы связи в кризисных ситуациях в сфере ИКТ, а также управления инцидентами и их урегулирования, в том числе путем принятия общих и транспарентных процессов, процедур и шаблонов[42].

Предложение о дополнительных действиях

- Рассмотреть возможность использования, сообразно обстоятельствам, таких многосторонних каналов связи на дипломатическом и техническом уровнях, таких как Глобальный реестр контактных пунктов, для обмена информацией или реагирования на запросы об оказании помощи в случае инцидента в сфере ИКТ.

[39] A/76/135, п. 53. Дополнительное примечание: такие структуры и механизмы могут включать: национальный центр или ответственное агентство или головное ведомство по вопросам безопасности ИКТ; и/или группы реагирования на компьютерные инциденты (CERTs) или группы реагирования на инциденты в сфере компьютерной безопасности (CSIRTs).
[40] A/76/135, пп. 51 и 52.
[41] A/76/135, п. 52.
[42] A/76/135, пп. 54 и 55.

Норма i)
Государства должны принимать разумные меры для обеспечения целостности каналов поставок, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование скрытых вредоносных функций.

Добровольные практические действия по реализации этой нормы

Действия на национальном уровне

☐ 1. Создать на национальном уровне всеобъемлющие, прозрачные, объективные и беспристрастные рамки и механизмы для управления рисками в отношении каналов поставок в соответствии с международными обязательствами государств с учетом целого ряда факторов, в том числе преимуществ и рисков, связанных с новыми технологиями[43].

☐ 2. Разработать стратегии и программы, направленные 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 выбору[44].

☐ 3. Принять меры по укреплению целостности каналов поставок, включая требования к поставщикам ИКТ учитывать вопросы безопасности и защиты ИКТ-продуктов при их проектировании и разработке, а также на протяжении всего их жизненного цикла. Рассмотреть вопрос о создании независимых и беспристрастных процессов сертификации[45].

☐ 4. Принять законодательные и другие гарантии, повышающие уровень защиты данных и конфиденциальности[46].

☐ 5. Принять меры, запрещающие внедрение скрытых вредоносных функций и использование уязвимостей в ИКТ-продуктах, которые могут поставить под угрозу конфиденциальность, целостность и доступность систем и сетей, в том числе критически важной инфраструктуры[47].

☐ 6. Укреплять партнерство с частным сектором для совместного повышения уровня безопасности ИКТ и их использования. Продолжать 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[48].

[43] A/76/135, п. 57 a).
[44] Второй ежегодный доклад о проделанной работе (A/78/265), п. 23 d).
[45] A/76/135, п. 58 a).
[46] A/76/135, п. 58 b).
[47] A/76/135, п. 58 c).
[48] Второй ежегодный доклад о проделанной работе (A/78/265), п. 23 e).

Действия, требующие международного сотрудничества

☐ 7. Уделять повышенное внимание в национальной политике и в диалоге с государствами и соответствующими субъектами в Организации Объединенных Наций и на других площадках вопросу о том, как обеспечить всем государствам возможность равноправно конкурировать и внедрять инновации, с тем чтобы создать условия для полной реализации ИКТ в целях ускорения глобального социального и экономического развития и содействия поддержанию международного мира и безопасности при одновременном обеспечении национальной безопасности и общественных интересов[49].

☐ 8. Участвовать в инклюзивных, транспарентных многосторонних процессах по принятию совместных мер, таких как обмен передовым опытом в области управления рисками в цепочках поставок; разработка и внедрение совместимых на глобальном уровне общих правил и стандартов обеспечения безопасности каналов поставок; и применение других подходов, направленных на снижение уровня уязвимости каналов поставок[50].

[49] A/76/135, п. 57 c).

[50] Второй ежегодный доклад о проделанной работе (A/78/265), п. 23 d).

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

Добровольные практические действия по реализации этой нормы

Действия на национальном уровне

☐ 1. Принять политику и программы раскрытия информации об уязвимостях, включая скоординированный процесс раскрытия информации об уязвимостях, чтобы свести к минимуму вред, наносимый обществу уязвимыми продуктами, и систематизировать отчетность об уязвимостях ИКТ[51].

☐ 2. Разработать в консультации с соответствующими отраслевыми и другими субъектами, занимающимися вопросами безопасности ИКТ, согласующиеся с соответствующими международными техническими стандартами руководящие принципы и стимулирующие меры, которые касаются:

- ответственной координации работы с уязвимостями и составления соответствующей отчетности, а также соответствующих ролей и обязанностей различных заинтересованных сторон в процессе представления отчетности;
- типов технической информации, подлежащих раскрытию или публичному распространению, включая обмен технической информацией о серьезных инцидентах в области использования ИКТ; и
- способов работы с конфиденциальными данными и обеспечения безопасности и конфиденциальности информации[52].

☐ 3. Принять меры, способствующие международному сотрудничеству в области ответственного информирования об уязвимостях ИКТ, включая направление запросов об оказании помощи между странами и группами реагирования на чрезвычайные ситуации, в соответствии с национальным законодательством[53].

☐ 4. Принять меры правовой защиты для исследователей и тестеров проникновения[54].

Действия, требующие международного сотрудничества

☐ 5. Принять беспристрастные правовые рамки, стратегии и программы, которыми можно было бы руководствоваться при принятии решений по устранению факторов уязвимостей ИКТ и ограничить их коммерческое распространение, что выступит средством защиты от любого ненадлежащего использования[55].

☐ 6. Использовать существующие многосторонние, региональные и субрегиональные органы и другие соответствующие каналы и платформы с участием различных заинтересованных сторон для выработки общего понимания относительно механизмов и процессов ответственного раскрытия информации об уязвимости[56].

---

[51] A/76/135, п. 61.
[52] A/76/135, п. 63.
[53] A/76/135, п. 61.
[54] A/76/135, п. 62.
[55] A/76/135, п. 62.
[56] A/76/135, п. 64.

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

Добровольные практические действия по реализации этой нормы

Действия на национальном уровне

☐ 1. Рассмотреть возможность отнесения CERTs/CSIRTs к категории национальной критически важной инфраструктуры[57].

☐ 2. Создать национальную рамочную систему управления инцидентами в сфере использования ИКТ с определенными функциями и обязанностями, в том числе для CERTs/CSIRTs для содействия сотрудничеству и координации между такими группами и другими соответствующими органами по вопросам безопасности и техническими органами на национальном, региональном и международном уровнях[58].

☐ 3. Включить в национальную рамочную систему управления инцидентами в сфере использования ИКТ политику, меры регулирования или процедуры, которые проясняют статус, полномочия и мандаты CERTs/CSIRTs и отделяют уникальные функции таких групп от других функций правительства[59].

☐ 4. Рассмотреть возможность публичного объявления или принятия мер, подтверждающих, что уполномоченные группы экстренного реагирования не будут использоваться для участия в злонамеренной международной деятельности, а также признать и уважать сферы деятельности и этические принципы, которыми руководствуются в своей работе уполномоченные группы экстренного реагирования[60].

Действия, требующие международного сотрудничества

☐ 5. Содействовать сотрудничеству и координации между CERTs/CSIRTs и другими соответствующими органами по вопросам безопасности и техническими органами на национальном, региональном и международном уровнях, в том числе с помощью национальных рамочных систем управления инцидентами в области безопасности ИКТ[61].

[57] A/76/135, п. 66.
[58] A/76/135, п. 68.
[59] A/76/135, п. 68.
[60] A/76/135, п. 67.
[61] A/76/135, п. 68.

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) 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;

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;

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

[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]

В дополнение к перечисленным выше глобальным МД государства включили следующие дополнительные добровольные глобальные МД:

МД 5. Содействовать обмену информацией о сотрудничестве и партнерстве между государствами в целях наращивания потенциала в области обеспечения безопасности ИКТ и активного применения МД

Программы по наращиванию потенциала являются важным направлением сотрудничества, которое может способствовать укреплению отношений и доверия в отношениях между государствами.

МД 6. Участвовать в регулярной организации семинаров, практикумов и учебных программ по вопросам безопасности ИКТ

Регулярная организация семинаров, практикумов и учебных программ по актуальным вопросам, связанным с безопасностью ИКТ, при широком представительстве государств могла бы способствовать укреплению связей и взаимопонимания и содействовать укреплению доверия.

МД 7. Вести обмен информацией и передовым опытом, в частности, по вопросам защиты критически важной инфраструктуры (КВИ) и критически важной информационной инфраструктуры (КВИИ), в том числе посредством наращивания потенциала в этой сфере

Обмен информацией и передовым опытом, в частности, по вопросам защиты критически важной инфраструктуры (КВИ) и критически важной информационной инфраструктуры (КВИИ), в том числе посредством наращивания потенциала в этой сфере, мог бы способствовать укреплению доверия в отношениях между государствами.

МД 8. Укрепление частно-государственного партнерства и сотрудничества в вопросах обеспечения безопасности ИКТ

Для выявления инцидентов в сфере использования ИКТ, защиты от них, реагирования на них и восстановления после них требуется целый ряд технических возможностей и знаний. В этой связи частно-государственное партнерство и сотрудничество, включая регулярный диалог и обмен передовым опытом, могли бы способствовать укреплению доверия.

Приложение C

Элементы открытого прикладного постоянного механизма по безопасности ИКТ в контексте международной безопасности

1. В настоящем документе изложены элементы для создания в Организации Объединенных Наций будущего постоянного механизма по безопасности ИКТ в контексте международной безопасности после завершения деятельности Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021-2025 годов. Постоянный механизм будет открытым и будет ориентирован на принятие конкретных мер; в основу его работы будут положены консенсусные договоренности о рамках ответственного поведения государств в области использования ИКТ, содержащиеся в предыдущих докладах РГОС и ГПЭ[1], в целях дальнейшего содействия созданию открытой, безопасной, стабильной, доступной, мирной и взаимосовместимой ИКТ-среды[2].

2. В развитие целей, которые были установлены в соответствующих резолюциях Генеральной Ассамблеи, включая, в частности, резолюции 78/16 и 78/237, касающиеся обсуждения вопроса о регулярном институциональном диалоге в рамках РГОС, государства рекомендовали создать будущий постоянный механизм на основе консенсусных элементов, содержащихся в настоящем документе, чтобы обеспечить плавный переход к новому механизму.

Руководящие принципы

3. В процессе создания будущего постоянного механизма будут учитываться элементы, рекомендованные консенсусом в рамках РГОС, включая приведенные ниже общие элементы, рекомендованные консенсусом в пунктах 55-57 второго ежегодного доклада РГОС о проделанной работе.

4. Будущий постоянный механизм будет основан 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.

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

[1] Второй ежегодный доклад о проделанной работе, п. 55 c).
[2] Второй ежегодный доклад о проделанной работе, п. 55 b).

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

7. Государства признали, что региональные и субрегиональные организации могли бы и далее 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 региональных организаций и не все региональные организации делают упор на вопросы безопасности в области использования ИКТ, государства отметили, что прилагаемые на региональном уровне усилия служат дополнением к работе будущего постоянного механизма[3].

Функции и объем работы

8. Будущий постоянный механизм будет заниматься вопросами безопасности ИКТ в контексте международной безопасности с целью содействия созданию открытой, безопасной, стабильной, доступной, мирной и взаимодополняемой ИКТ-среды.

9. Обеспечивая преемственность и опираясь на результаты деятельности рабочей группы открытого состава 2021-2025 годов и предыдущие договоренности РГОС и ГПЭ, открытый прикладной постоянный механизм будет выполнять такие функции, как наращивание потенциала всех государств в области обеспечения безопасности ИКТ, включая разработку и внедрение кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ; содействие внедрению кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ; дальнейшее развитие кумулятивных и эволюционирующих рамок ответственного поведения государств в области использования ИКТ; рассмотрение — с учетом перечисленных выше функций и путем содействия проведению комплексных, ориентированных на политику и сквозных обсуждений — таких вопросов, как существующие и потенциальные угрозы; добровольные, не имеющие обязательной силы нормы ответственного поведения государств и способы их реализации при том понимании, что со временем могут быть разработаны дополнительные нормы; а также дальнейшее изучение вопроса о том, как нормы международного права применяются к использованию ИКТ, отмечая возможность будущей разработки дополнительных имеющих обязательную силу юридических обязательств, если это будет необходимо, рассмотрение вопроса о том, существуют ли какие-либо пробелы в сфере применения действующих норм международного права к использованию ИКТ, и дальнейшее рассмотрение вопроса о разработке дополнительных имеющих обязательную силу юридических обязательств[4]; разработка и реализация меры укрепления доверия; а также разработка и реализация мер по наращиванию потенциала.

10. С учетом функций будущего постоянного механизма, государства признали, что международное сотрудничество и помощь могут играть существенно важную роль в обеспечении государствами безопасности ИКТ и их мирного использования[5]. Кроме того, поскольку наращивание потенциала затрагивает все

[3] Первый ежегодный доклад о проделанной работе (A/77/275), п. 5 и второй ежегодный доклад о проделанной работе (A/78/265), п. 7.

[4] Второй ежегодный доклад о проделанной работе, п. 32.

[5] Доклад ГПЭ 2015 года, п. 19.

вопросы безопасности ИКТ и выступает в качестве фактора, способствующего повышению устойчивости ИКТ и укрепления способности государств выявлять злонамеренную деятельность в сфере использования ИКТ, обеспечивать защиту от такой деятельности или реагировать на нее, одной из важных функций будущего постоянного механизма станет реализация таких ориентированных на конкретные действия подходов к наращиванию потенциала, как согласование потребностей с ресурсами и технической помощью. Кроме того, государства признают, что наращивание потенциала необходимо и для того, чтобы государства могли участвовать в работе будущего постоянного механизма на инклюзивной основе и на равных условиях.

11. Будущий постоянный механизм будет способствовать взаимодействию и сотрудничеству с заинтересованными сторонами и субъектами, включая представителей деловых кругов, неправительственных организаций и научного сообщества, посредством изучения и использования опыта процесса РГОС. Участие других заинтересованных сторон и субъектов, включая представителей деловых кругов, неправительственных организаций и научного сообщества, в работе будущего постоянного механизма будет определяться:

a) целью содействия проведению инклюзивных обсуждений в рамках будущего постоянного механизма с опорой на соответствующий опыт для поддержки работы механизма сообразно обстоятельствам;

b) возможностями, которые основные пленарные заседания, специальные тематические группы, специальные межсессионные совещания и обзорные конференции будут обеспечивать для проведения консультаций между государствами и другими заинтересованными сторонами и субъектами, включая представителей деловых кругов, неправительственных организаций и научного сообщества;

c) всеобъемлющим принципом, согласно которому будущий постоянный механизм будет иметь в своей основе направляемый государствами процесс, в рамках которого проведение переговоров и принятие решений по вопросам безопасности ИКТ останутся прерогативой государств;

d) вынесенной в адрес государств рекомендацией продолжить обсуждения в рамках нынешней РГОС и представить в заключительном докладе РГОС, который будет принят в июле 2025 года, рекомендации относительно условий участия в будущем постоянном механизме других заинтересованных сторон и субъектов, включая представителей деловых кругов, неправительственных организаций и научного сообщества.

Структура

12. Будущий постоянный механизм будет иметь пятилетний цикл, состоящий из двух двухгодичных циклов и последующего годичного обзорного цикла. Заседания будущего постоянного механизма проходят в следующих форматах:

a) **основные пленарные заседания**. Ежегодно в течение каждого двухгодичного цикла будет созываться одно основное пленарное заседание продолжительностью не менее одной недели. На основных пленарных заседаниях будут проводиться обсуждения в соответствии с функциями и объемом работы, изложенными выше, а также рассматриваться работа и рекомендации целевых тематических групп;

b) **специальные тематические группы**. Специальные тематические группы будут создаваться в соответствии с решениями будущего постоянного механизма для проведения целенаправленных обсуждений, при наличии такой

необходимости. Специальные тематические группы будут представлять основным пленарным заседаниям доклады, содержащие обновленную информацию и рекомендации. Государствам рекомендуется продолжить обсуждение в рамках нынешней РГОС вопроса о специальных тематических группах будущего постоянного механизма и представить рекомендации в заключительном докладе РГОС, который будет принят в июле 2025 года;

c) **специальные межсессионные совещания**. Председатель будущего постоянного механизма на основе консультаций с государствами мог бы также созывать специальные межсессионные совещания для проведения дополнительных обсуждений по конкретным вопросам или для обсуждения докладов и рекомендаций, при наличии такой необходимости;

d) **обзорная конференция**. Обзорная конференция будет созываться раз в пять лет для обзора эффективного функционирования будущего постоянного механизма и определения стратегических направлений и директивных указаний для основных пленарных заседаний и специальных тематических групп на последующие четыре года. Кроме того, в ходе обзорной конференции государства могут также принимать решения на основе консенсуса по любым изменениям элементов будущего постоянного механизма, содержащихся в настоящем документе.

13. В каждом двухгодичном цикле будущий постоянный механизм будет возглавлять Председатель, избираемый на два года на основе справедливого географического представительства. Кроме того, на основе справедливого географического представительства будет избираться Председатель на один год для руководства процессом годичной обзорной конференции.

14. Для содействия инклюзивному участию заседания будущего постоянного механизма, включая основные пленарные заседания, заседания любых специальных тематических групп и специальные межсессионные совещания, не будут проводиться параллельно, при этом некоторые заседания могут быть созваны в гибридном формате.

Порядок работы

15. Будущий постоянный механизм будет работать следующим образом:

a) постоянный механизм будет создан в качестве вспомогательного органа Генеральной Ассамблеи Организации Объединенных Наций, подотчетного Первому комитету;

b) функции секретариата постоянного механизма будет выполнять Управление по вопросам разоружения;

c) будет создан электронный портал и/или веб-сайт для поддержки и облегчения работы постоянного механизма;

d) Глобальный реестр контактных пунктов будет служить добровольным постоянным инструментом для использования государствами;

e) официальные заседания постоянного механизма будут созываться в Центральных учреждениях Организации Объединенных Наций в Нью-Йорке.

16. Для обеспечения плавного перехода от работы РГОС к будущему постоянному механизму государства рекомендуют принять следующие меры:

a) созыв организационной сессии не позднее марта 2026 года для проведения, в частности i) выборов Председателя будущего постоянного механизма, ii) утверждения повестки дня, iii) создания специальных тематических групп и iv) утверждения других необходимых рабочих процедур;

b) созыв первого основного пленарного заседания не позднее июня 2026 года.

Принятие решений

17. Будущий постоянный механизм будет принимать все решения на основе принципа консенсуса. На основе консультаций с государствами решения мог бы предлагать Председатель для принятия государствами на основе консенсуса в любое время в ходе основного пленарного заседания, а официальное утверждение решений должно происходить сразу же после их принятия будущим постоянным механизмом.