Организация Объединенных Наций A/C.1/73/L.27

Генеральная Ассамблея

Distr.: Limited
22 October 2018
Russian
Original: English

Семьдесят третья сессия
Первый комитет
Пункт 96 повестки дня
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Азербайджан, Алжир, Ангола, Беларусь, Боливия (Многонациональное Государство), Бурунди, Венесуэла (Боливарианская Республика), Демократическая Республика Конго, Зимбабве, Казахстан, Камбоджа, Китай, Корейская Народно-Демократическая Республика, Куба, Мадагаскар, Намибия, Непал, Никарагуа, Пакистан, Российская Федерация, Самоа, Сирийская Арабская Республика, Суринам, Сьерра-Леоне, Таджикистан, Узбекистан и Эритрея: проект резолюции

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Генеральная Ассамблея,

ссылаясь на свои резолюции 36/103 от 9 декабря 1981 года, 43/78 H от 7 декабря 1988 года, 53/70 от 4 декабря 1998 года, 54/49 от 1 декабря 1999 года, 55/28 от 20 ноября 2000 года, 56/19 от 29 ноября 2001 года, 57/53 от 22 ноября 2002 года, 58/32 от 8 декабря 2003 года, 59/61 от 3 декабря 2004 года, 60/45 от 8 декабря 2005 года, 61/54 от 6 декабря 2006 года, 62/17 от 5 декабря 2007 года, 63/37 от 2 декабря 2008 года, 64/25 от 2 декабря 2009 года, 65/41 от 8 декабря 2010 года, 66/24 от 2 декабря 2011 года, 67/27 от 3 декабря 2012 года, 68/243 от 27 декабря 2013 года, 69/28 от 2 декабря 2014 года, 70/237 от 23 декабря 2015 года и 71/28 от 5 декабря 2016 года,

отмечая значительный прогресс, достигнутый в разработке и внедрении новейших информационных технологий и средств телекоммуникации,

подтверждая, что информационно-коммуникационные технологии являются технологиями двойного назначения, которые могут использоваться как в законных, так и в злонамеренных целях,

выражая обеспокоенность по поводу того, что ряд государств наращивают потенциал в области использования информационно-коммуникационных технологий в военных целях и что использование таких технологий в будущих конфликтах между государствами становится более вероятным,

подчеркивая, что интересам всех государств отвечает поощрение использования информационно-коммуникационных технологий в мирных целях, в интересах построения общего будущего для всего человечества в киберпространстве и что государства также заинтересованы в предотвращении конфликтов, возникающих в результате использования информационно-коммуникационных технологий,

отмечая, что Организация Объединенных Наций должна играть ведущую роль в поощрении диалога между государствами-членами для выработки общего понимания в сфере безопасности и использования информационно-коммуникационных технологий, а также в выработке общего понимания в вопросах применимости норм международного права и норм, правил и принципов ответственного поведения государств в этой сфере, поощрять региональные усилия, меры по укреплению доверия и повышению транспарентности, а также способствовать наращиванию потенциала и распространению передового опыта,

выражая обеспокоенность по поводу того, что встроенные скрытые вредоносные функции могут использоваться в сфере информационно-коммуникационных технологий таким образом, что это негативно скажется на безопасном и надежном использовании таких технологий и на каналах поставок товаров и услуг, связанных с информационно-коммуникационными технологиями, подорвет доверие в торговле и нанесет ущерб национальной безопасности,

считая необходимым предотвратить использование информационных ресурсов или технологий в преступных или террористических целях,

подчеркивая необходимость усиления координации и сотрудничества между государствами в борьбе с преступным злоупотреблением информационными технологиями и в этой связи подчеркивая роль, которую могут сыграть Организация Объединенных Наций и другие международные и региональные организации,

подчеркивая также важность уважения прав человека и основных свобод при использовании информационно-коммуникационных технологий,

приветствуя результативную работу Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и подготовленные соответствующие итоговые доклады, препровожденные Генеральным секретарем[1],

с удовлетворением отмечая, что при рассмотрении вопроса о применимости норм международного права к использованию информационно-коммуникационных технологий государствами Группа правительственных экспертов в своем докладе за 2015 год[2] определила, что важнейшее значение имеют обязанности государств в соответствии со следующими принципами Устава Организации Объединенных Наций и другими нормами международного права: суверенное равенство; разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость; отказ в 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 Организации Объединенных Наций; уважение прав человека и основных свобод; невмешательство во внутренние дела других государств,

[1] A/65/201, A/68/98 и A/70/174.
[2] A/70/174.

подтверждая содержащийся в докладах Группы правительственных экспертов 2013[3] и 2015 годов[2] вывод о том, что международное право, и в частности Устав Организации Объединенных Наций, применимо и имеет важное значение для поддержания мира и стабильности и создания открытой, безопасной, стабильной, доступной и мирной информационной среды, что добровольные и необязывающие нормы, правила и принципы ответственного поведения государств в сфере использования информационно-коммуникационных технологий могут снизить риск нарушения международного мира, безопасности и стабильности и что с учетом уникальных особенностей информационно-коммуникационных технологий со временем могут быть разработаны дополнительные нормы,

подтверждая также, что государственный суверенитет и международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами деятельности, связанной с информационно-коммуникационными технологиями, и к их юрисдикции над объектами инфраструктуры информационно-коммуникационных технологий в пределах их территории,

отмечая, что наращивание потенциала имеет существенно важное значение для сотрудничества государств и укрепления доверия в области безопасности информационно-коммуникационных технологий,

подчеркивая необходимость активизации усилий по преодолению отставания в сфере цифровых технологий путем облегчения передачи информационных технологий развивающимся странам и наращивания их потенциала в вопросах передовой практики и профессиональной подготовки в области кибербезопасности, в соответствии с резолюцией 64/211 Генеральной Ассамблеи от 21 декабря 2009 года, озаглавленной «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур»,

особо отмечая, что, хотя главная ответственность за обеспечение безопасности и мирной информационно-коммуникационной среды лежит на государствах, выявление механизмов вовлечения, при необходимости, организаций гражданского общества, частного сектора и научных кругов могло бы способствовать повышению эффективности международного сотрудничества,

1. *принимает* следующий проект международного кодекса поведения для обеспечения международной информационной безопасности:

1. Государства должны соблюдать Устав Организации Объединенных Наций и регулирующие международные отношения общепризнанные нормы международного права, которые включают, в частности, уважение суверенитета, территориальной целостности и политической независимости всех государств, уважение прав человека и основных свобод, а также уважение многообразия истории, культуры и социального устройства всех стран.

2. В соответствии с целями Устава Организации Объединенных Наций, в том числе для поддержания международного мира и безопасности, государства должны сотрудничать в разработке и осуществлении мер по повышению стабильности и безопасности в использовании информационно-коммуникационных технологий и предупреждению совершения в сфере таких технологий действий, признаваемых вредоносными или способных создавать угрозу международному миру и безопасности.

[3] A/68/98.

3. Государства не должны использовать информационно-коммуникационные технологии и информационно-коммуникационные сети для проведения мероприятий, которые идут вразрез с задачей поддержания международного мира и безопасности.

4. Государства не должны использовать информационно-коммуникационные технологии и информационно-коммуникационные сети для вмешательства во внутренние дела других государств или с целью подрыва их политической, экономической и социальной стабильности и подтверждают право и обязанность государств бороться, в рамках своих конституционных прав, с распространением ложных или искаженных новостных сообщений, которые могут быть истолкованы как вмешательство во внутренние дела других государств или как нанесение вреда поощрению мира, сотрудничества и дружественных отношений между государствами и народами.

5. Государства должны признать, что государства несут обязанность воздерживаться от любых клеветнических кампаний, диффамации или враждебной пропаганды с целью вмешательства во внутренние дела других государств.

6. Государства должны прилагать усилия для обеспечения безопасности товаров и услуг, связанных с информационно-коммуникационными технологиями, на всех уровнях каналов поставки в целях недопущения того, чтобы другие государства использовали свое доминирующее положение в сфере информационно-коммуникационных технологий, в том числе доминирование в сфере ресурсов, важнейших элементов инфраструктуры, основных технологий, товаров и услуг, связанных с информационно-коммуникационными технологиями, и информационно-коммуникационных сетей, для подрыва права государств на независимый контроль товаров и услуг, связанных с информационно-коммуникационными технологиями, или создания угрозы политической, экономической и социальной безопасности государств.

7. Государства должны подтвердить вытекающие из соответствующих норм и правил права и обязанности всех государств в отношении правовой защиты своего информационного пространства и критически важных объектов информационной инфраструктуры от ущерба, вызванного угрозами, вмешательством, нападениями и актами саботажа.

8. Государства должны признать, что права личности в офлайновой среде должны также защищаться и в онлайновой среде; и полностью уважать права и свободы в информационном пространстве, в том числе право и свободу искать, получать и распространять информацию, принимая во внимание тот факт, что в статье 19 Международного пакта о гражданских и политических правах[4] это право увязывается с особыми обязанностями и особой ответственностью. Следовательно, оно может подлежать некоторым ограничениям, которые, однако, должны быть установлены законом и являться необходимыми:

a) для уважения прав или репутации других лиц;

b) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения.

9. Все государства должны играть одинаковую роль и нести равную ответственность за международное управление Интернетом, обеспечение

[4] См. резолюцию 2200 A (XXI), приложение.

безопасности, бесперебойности и стабильности его функционирования и его развитие таким образом, который поощряет создание многосторонних, транспарентных и демократических международных механизмов управления Интернетом, позволяющих обеспечивать справедливое распределение ресурсов, способствовать доступу для всех и гарантировать стабильное и безопасное функционирование Интернета.

10. Государства должны выполнять свои международные обязательства в отношении международно-противоправных деяний, присваиваемых им в соответствии с международным правом. Вместе с тем указание на то, что та или иная деятельность в области информационно-коммуникационных технологий была начата или иным образом происходит с территории или объектов информационно-коммуникационной инфраструктуры государства, может быть недостаточным для присвоения этой деятельности такому государству. Государства должны принять к сведению, что обвинение в организации и совершении противоправных деяний, выдвигаемые против государств, должны быть обоснованными. В случаях инцидентов в сфере информационно-коммуникационных технологий государства должны учитывать всю соответствующую информацию, в том числе более общий контекст события, проблемы присвоения ответственности в информационно-коммуникационной среде, а также характер и масштабы последствий.

11. Государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием информационно-коммуникационных технологий. Государства не должны использовать посредников для совершения международно-противоправных деяний с использованием информационно-коммуникационных технологий и должны стремиться обеспечивать, чтобы их территория не использовалась негосударственными субъектами для совершения таких деяний.

12. Государства должны рассмотреть вопрос о наиболее эффективных способах сотрудничества в обмене информацией, оказании взаимопомощи, преследовании лиц, виновных в использовании информационно-коммуникационных технологий в террористических и преступных целях, и сдерживании распространения информации, разжигающей терроризм, сепаратизм и экстремизм или обостряющей ненависть на этнической, расовой или религиозной почве, и осуществлять другие совместные меры по устранению таких угроз. Государствам, возможно, потребуется рассмотреть вопрос о необходимости разработки новых мер в этой области.

13. В процессе обеспечения безопасного использования информационно-коммуникационных технологий государства должны соблюдать положения резолюций Совета по правам человека 20/8 от 5 июля 2012 года[5] и 26/13 от 26 июня 2014 года[6] о поощрении, защите и осуществлении прав человека в Интернете и резолюций Генеральной Ассамблеи 68/167 от 18 декабря 2013 года и 69/166 от 18 декабря 2014 года о праве на неприкосновенность личной жизни в эпоху цифровых технологий, чтобы обеспечить всестороннее уважение прав человека, включая право свободно выражать свое мнение.

14. Государство не должно осуществлять или заведомо поддерживать деятельность в сфере информационно-коммуникационных технологий, если

[5] См. *Официальные отчеты Генеральной Ассамблеи, шестьдесят седьмая сессия, Дополнение № 53 и исправление* (A/67/53 и A/67/53/Corr.1), глава IV, раздел A.

[6] Там же, шестьдесят девятая сессия, Дополнение № 53 (A/69/53), глава V, раздел A.

такая деятельность противоречит его обязательствам по международному праву, наносит преднамеренный ущерб критически важным объектам инфраструктуры или иным образом препятствует использованию и функционированию критически важных объектов инфраструктуры для обслуживания населения.

15. Государства должны принимать надлежащие меры для защиты критически важных объектов своей инфраструктуры от угроз в сфере информационно-коммуникационных технологий, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи от 23 декабря 2003 года о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции.

16. Государства должны отвечать на соответствующие просьбы об оказании помощи, поступающие от других государств, критически важные объекты инфраструктуры которых становятся объектом злонамеренных действий с применением информационно-коммуникационных технологий. Государства должны также удовлетворять соответствующие просьбы о смягчении последствий злонамеренных действий в сфере информационно-коммуникационных технологий, направленных против критически важных объектов инфраструктуры других государств, если такие действия проистекают с их территории, надлежащим образом принимая во внимание вопросы суверенитета.

17. Государства должны принимать разумные меры для обеспечения неприкосновенности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов информационно-коммуникационных технологий, обеспечения неприкосновенности права государств на независимый контроль в области товаров и услуг, связанных с информационно-коммуникационными технологиями, и защиты от угроз их политической, экономической и социальной безопасности.

18. Государства должны стремиться предупреждать распространение вредоносных программных и технических средств в сфере информационно-коммуникационных технологий и использование скрытых вредоносных функций.

19. Государства должны поощрять ответственное представление информации о факторах уязвимости в сфере информационно-коммуникационных технологий и делиться соответствующей информацией о существующих способах устранения таких факторов уязвимости, чтобы ограничить, а по возможности и устранить потенциальные угрозы для информационно-коммуникационных технологий и объектов инфраструктуры, зависящих от таких технологий.

20. Государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренного реагирования (известных также как группы реагирования на чрезвычайные ситуации в компьютерной сфере и группы по реагированию на инциденты в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренного реагирования для осуществления злонамеренной международной деятельности.

21. Государства должны поощрять частный сектор и гражданское общество к тому, чтобы они играли соответствующую роль в укреплении безопасности и безопасности использования информационно-коммуникационных технологий, включая каналы поставки товаров и услуг, связанных с

информационно-коммуникационными технологиями. Государства должны сотрудничать с частным сектором и организациями гражданского общества в области применения норм ответственного поведения в информационном пространстве с учетом их потенциальной роли.

22. Государства должны разрабатывать меры по укреплению доверия, направленные на повышение предсказуемости и снижение вероятности недоразумений и риска возникновения конфликта. Такие меры будут включать в себя, в частности, добровольный обмен информацией о национальных стратегиях и организационных структурах по обеспечению информационной безопасности государства, публикацию «белых книг» и обмен передовым опытом, если это практически возможно и целесообразно.

23. Государства должны оказывать развивающимся странам помощь в их усилиях по дальнейшему наращиванию потенциала в области информационной безопасности и по преодолению отставания в сфере цифровых технологий.

24. Государства должны укреплять двустороннее, региональное и международное сотрудничество, способствовать тому, чтобы Организация Объединенных Наций играла более значимую роль в таких сферах, как поощрение разработки международно-правовых норм в области информационной безопасности, мирное урегулирование международных споров, качественное улучшение международного сотрудничества в области информационной безопасности, а также укреплять координацию между соответствующими международными организациями.

25. Государства должны урегулировать любой спор, вытекающий из применения настоящего кодекса поведения, мирными средствами и воздерживаться от угрозы силой или ее применения;

2. *призывает* государства-члены далее содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также возможных стратегий по рассмотрению угроз, возникающих в этой сфере, исходя из необходимости сохранить свободный поток информации;

3. *полагает*, что целям таких стратегий соответствовало бы продолжение изучения соответствующих международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем;

4. *просит* все государства-члены продолжать, принимая во внимание оценки и рекомендации, содержащиеся в докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности[1], информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:

a) общая оценка проблем информационной безопасности;

b) усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области;

c) содержание концепций, упомянутых в пункте 3 выше;

d) возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне;

5. *просит* Генерального секретаря при содействии Группы правительственных экспертов, которая должна быть создана в 2019 году на основе справедливого географического распределения, продолжить, в качестве одной из задач первостепенной важности, разработку норм, правил и принципов ответственного поведения государств, перечисленных в пункте 1 выше, и путях их осуществления; представить при необходимости соответствующие изменения или разработать дополнительные правила поведения; изучить возможность установления регулярного институционального диалога с широким кругом участников под эгидой Организации Объединенных Наций; и продолжить в целях выработки общего понимания исследование существующих и потенциальных угроз в области информационной безопасности и возможных совместных мер по их устранению и того, как нормы международного права применяются к использованию информационно-коммуникационных технологий государствами, а также мер укрепления доверия и наращивания потенциала и концепций, упомянутых в пункте 3 выше, и представить доклад о результатах этого исследования Генеральной Ассамблее на ее семьдесят пятой сессии;

6. *постановляет* включить в предварительную повестку дня своей семьдесят четвертой сессии пункт, озаглавленный «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».