Организация Объединенных Наций A/68/98*

Генеральная Ассамблея

Distr.: General
24 June 2013
Russian
Original: English

Шестьдесят восьмая сессия
Пункт 94 предварительной повестки дня**
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

Записка Генерального секретаря

Генеральный секретарь имеет честь препроводить настоящим доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Эта группа была создана в соответствии с пунктом 4 резолюции 66/24 Генеральной Ассамблеи.

* Переиздано по техническим причинам 30 июля 2013 года.
** A/68/150.

13-37168* (R) 050813 060813

Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

Резюме

Появление информационно-коммуникационных технологий (ИКТ) оказало существенное воздействие на положение дел в области международной безопасности. Эти технологии позволяют получать огромные экономические и социальные выгоды. Они также могут использоваться в целях, несовместимых с поддержанием международного мира и безопасности, в силу чего в последние годы заметно повысился уровень риска в связи с использованием ИКТ для совершения преступлений и других подрывных действий. Злонамеренное использование ИКТ злоумышленниками, которые нередко действуют в условиях безнаказанности, легко скрыть, а выявление конкретного злоумышленника может быть сопряжено с трудностями. В результате создаются условия, в которых эти злоумышленники могут осуществлять все более сложные вредоносные действия.

Государства-члены неоднократно заявляли о необходимости совместных действий, направленных на ликвидацию угроз, обусловленных злонамеренным использованием ИКТ. Международное сотрудничество — важный фактор снижения рисков и укрепления безопасности. Дальнейший прогресс в деле налаживания сотрудничества на международном уровне требует принятия мер по созданию мирных, безопасных, открытых — и благоприятных для развития сотрудничества — условий для использования ИКТ. Совместные меры, которые могут повысить стабильность и укрепить безопасность, включают в себя нормы, правила и принципы ответственного поведения государств, добровольные меры по повышению транспарентности, укреплению доверия в межгосударственных отношениях и наращиванию потенциала. Государства должны играть лидирующую роль в этом процессе, вместе с тем активное участие частного сектора и гражданского общества могло бы способствовать повышению эффективности такого сотрудничества.

Признавая всеобъемлющий характер данной проблемы, учитывая существующие и потенциальные угрозы и руководствуясь рекомендациями, содержащимися в опубликованном в июле 2010 года докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/65/201), Группа правительственных экспертов представляет в настоящем докладе свои рекомендации по оказанию содействия укреплению мира и стабильности применительно к использованию государствами ИКТ.

В докладе отмечается, что применение норм, основанных на положениях международного права, в отношении деятельности государств, связанной с использованием ИКТ, — необходимая предпосылка для снижения риска нарушения международного мира, безопасности и стабильности. В докладе рекомендуется продолжать исследования в целях содействия формированию общего понимания того, как эти нормы применяются к поведению государств и использованию государствами ИКТ. В докладе говорится, что с учетом уникальных особенностей ИКТ со временем могут быть разработаны дополнительные нормы.

Доклад отражает сделанный Группой 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, мирной и доступной информационной среды. Группа также пришла к выводу, что государственный суверенитет и международные нормы и принципы, вытекающие из принципа государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием ИКТ, а также на юрисдикцию государств над ИКТ-инфраструктурой на их территории; государства должны выполнять свои международные обязательства в отношении приписываемых им международно противоправных деяний. В докладе содержатся рекомендации в отношении добровольных мер укрепления доверия и транспарентности, а также международного сотрудничества в сфере наращивания потенциала в области безопасности ИКТ, особенно в развивающихся странах. В соответствии с рекомендациями Группы регулярный институциональный диалог по этим вопросам под эгидой Организации Объединенных Наций, а также регулярный диалог в рамках других форумов будут способствовать повышению эффективности таких мер. Государства-члены должны внимательно изучить настоящий доклад и подумать над возможными путями доработки и осуществления указанных рекомендаций.

Содержание

Предисловие Генерального секретаря

В настоящее время информационно-коммуникационные технологии (ИКТ) являются непременным атрибутом повседневной жизни. И хотя все страны отдают должное значительным преимуществам ИКТ, получил широкое признание тезис о том, что неправильное использование таких технологий угрожает международному миру и безопасности.

В настоящем докладе содержатся разработанные Группой правительственных экспертов из 15 государств рекомендации по устранению связанных с использованием ИКТ существующих и потенциальных угроз со стороны государств, субъектов, действующих в их интересах, или негосударственных игроков. Настоящий доклад подготовлен на основе рекомендаций предыдущей группы экспертов, которые были приняты в 2010 году и включали в себя указание на необходимость дальнейшей проработки норм, регулирующих использование государствами ИКТ, способов повышения доверия и мер по укреплению потенциала.

Я с удовлетворением отмечаю, что в этом докладе подчеркивается ключевая роль Устава Организации Объединенных Наций и международного права, а также важность ответственного поведения государств. Содержащиеся в нем рекомендации указывают на то, как увязать вопросы безопасности ИКТ с существующими нормами международного права и договоренностями, которые регулируют межгосударственные отношения и служат основой для международного мира и безопасности.

Как отмечает Группа, Организация Объединенных Наций играет лидирующую роль в налаживании диалога между государствами-членами по проблеме безопасности в сфере использования ИКТ и в дальнейшем развитии международного сотрудничества в этой области.

Я благодарю Председателя Группы и экспертов за их добросовестный труд. Настоящий доклад станет прочной основой для будущих усилий по укреплению безопасности и стабильности в сфере использования ИКТ. Я передаю рекомендации Группы на рассмотрение Генеральной Ассамблее и считаю их важным шагом в направлении наращивания глобальных усилий по минимизации рисков, связанных с использованием ИКТ, и одновременному повышению их ценности.

Препроводительное письмо

7 июня 2013 года

Имею честь настоящим препроводить доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Эта Группа была создана в 2012 году в соответствии с пунктом 4 резолюции 66/24 Генеральной Ассамблеи. В качестве Председателя Группы я с удовлетворением сообщаю Вам, что по этому докладу был достигнут консенсус.

В своей резолюции, озаглавленной «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», Генеральная Ассамблея просила создать в 2012 году на основе справедливого географического распределения Группу правительственных экспертов, с тем чтобы продолжить исследование существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, включая нормы, правила или принципы ответственного поведения государств и меры укрепления доверия в информационном пространстве, а также концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем. Группе было также предложено принять во внимание оценки и рекомендации, содержащиеся в докладе предыдущей группы правительственных экспертов (A/65/201). К Генеральному секретарю была обращена просьба представить Генеральной Ассамблее на ее шестьдесят восьмой сессии доклад о результатах этого исследования.

В соответствии с положениями данной резолюции были назначены эксперты из 15 государств: Австралии, Аргентины, Беларуси, Германии, Египта, Индии, Индонезии, Канады, Китая, Российской Федерации, Соединенного Королевства Великобритании и Северной Ирландии, Соединенных Штатов Америки, Франции, Эстонии и Японии. Список экспертов приводится в приложении.

Группа провела всесторонний и углубленный обмен мнениями по вопросу о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности. Всего Группа провела три сессии: первую сессию с 6 по 10 августа 2012 года в Центральных учреждениях Организации Объединенных Наций; вторую — с 14 по 18 января 2013 года в Женеве; третью — с 3 по 7 июня в Центральных учреждениях Организации Объединенных Наций.

Группа хотела бы выразить свою признательность за внесенный вклад Институту Организации Объединенных Наций по исследованию проблем разоружения, который консультировал Группу и от которого в ее работе участвовали Джеймс Льюис, Керстин Вигнард (на второй и третьей сессиях) и Бен Бейсли Уокер (на первой сессии). Группа хотела бы также выразить свою признательность сотруднику Управления по вопросам разоружения Секретариата Юэну Бьюканану, который исполнял обязанности Секретаря Группы, и другим должностным лицам Секретариата, оказавшим содействие Группе.

(*Подпись*) Дебора **Стоукс**
Председатель Группы

I. Введение

1. Появление информационно-коммуникационных технологий (ИКТ) оказало существенное воздействие на положение дел в области международной безопасности. Эти технологии позволяют получать огромные экономические и социальные выгоды; они также могут использоваться в целях, несовместимых с поддержанием международного мира и безопасности. Уровень риска в последние годы заметно повысился в связи с использованием ИКТ для совершения преступлений и осуществления подрывной деятельности.

2. Международное сотрудничество является важным фактором снижения риска и укрепления безопасности. По этой причине Генеральная Ассамблея просила Генерального секретаря с помощью Группы правительственных экспертов продолжить изучение возможных совместных мер по устранению существующих и потенциальных угроз (резолюция 66/24) и представить доклад о результатах этой работы на шестьдесят восьмой сессии Ассамблеи. Настоящий доклад подготовлен на основе доклада 2010 года (A/65/201), подготовленного предыдущей группой правительственных экспертов, которая рассмотрела эту тему и вынесла рекомендации относительно дальнейшей работы.

3. В докладе 2010 года государствам было рекомендовано продолжать диалог в целях обсуждения норм, касающихся использования государствами ИКТ, уменьшения коллективного риска и защиты критически важной национальной и международной инфраструктуры. Группа призвала принимать меры по укреплению доверия, обеспечению стабильности и уменьшению риска, включая обмен национальными мнениями по вопросу об использовании ИКТ в конфликтах, и осуществлять обмен информацией о национальных законах, стратегиях обеспечения безопасности ИКТ, а также о соответствующих технологиях, принципах и передовых методах. В докладе 2010 года была подчеркнута важность создания потенциала в государствах, которым может потребоваться помощь в обеспечении безопасности их ИКТ, и было рекомендовано продолжить работу по выработке общей терминологии и определений.

4. Многочисленные двусторонние, региональные и многосторонние инициативы, осуществленные после 2010 года, свидетельствуют о том, что сейчас все большее значение придается укреплению безопасности при использовании ИКТ и самих ИКТ, снижению рисков для общественной безопасности, укреплению безопасности государств и упрочению глобальной стабильности. Все страны заинтересованы в поощрении использования ИКТ в мирных целях. Страны также заинтересованы в предотвращении конфликтов, возникающих в результате использования ИКТ. Общее понимание в отношении норм, правил и принципов, применимых к использованию ИКТ государствами, и добровольные меры укрепления доверия могут играть важную роль в поддержании мира и безопасности. Несмотря на то что деятельность международного сообщества по противодействию этой угрозе международному миру и безопасности находится на начальном этапе, тем не менее уже сейчас можно наметить для дальнейшего рассмотрения ряд мер, касающихся норм, правил и принципов ответственного поведения государств.

Угрозы, риски и факторы уязвимости

5. ИКТ являются технологиями двойного назначения, которые могут использоваться как в законных, так и в злонамеренных целях. Любое устройство ИКТ может стать источником или объектом злонамеренных действий. Злонамеренное использование ИКТ легко скрыть, а выявление конкретного злоумышленника может быть сопряжено с трудностями, в связи с чем злоумышленники, которые нередко действуют в условиях безнаказанности, могут осуществлять все более сложные вредоносные действия. Эту проблему также усугубляет глобальный охват сетей ИКТ. Глобальный доступ, уязвимые технологии и фактор анонимности облегчают использование ИКТ в целях осуществления подрывной деятельности.

6. Угрозы частным лицам, компаниям, национальной инфраструктуре и государственным органам приобретают все более острый характер, и соответствующие инциденты имеют все более тяжелые последствия. В качестве источников таких угроз выступают как государственные, так и негосударственные субъекты. Кроме того, отдельные лица, группы или организации, включая преступные сообщества, совершающие злонамеренные действия, связанные с использованием ИКТ, могут действовать в интересах государств. Возможность создания и широкомасштабного применения государствами или негосударственными субъектами сложных вредоносных инструментов и средств — таких, например, как бот-сети — повышает риск ошибочной идентификации и непреднамеренной эскалации. Отсутствие общих представлений о приемлемом поведении государства в вопросах использования ИКТ ведет к усилению угрозы международному миру и безопасности.

7. Террористические группы используют ИКТ для поддержания контактов, сбора информации, вербовки сторонников, организации, планирования и координации террористических актов, пропаганды своих идей и действий и сбора финансовых средств. Если такие группы получат в свое распоряжение средства нападения, они смогут вести подрывную деятельность с помощью ИКТ.

8. Государства обеспокоены возможностью включения в ИКТ скрытых вредоносных функций, которые могут использоваться для подрыва безопасности и надежности использования ИКТ и всей системы производства и сбыта информационных товаров и информационно-технических услуг, а также для подрыва доверия между контрагентами в сфере торговли и причинения ущерба национальной безопасности.

9. Более широкое использование ИКТ на ключевых инфраструктурных объектах и в системах управления производственными процессами открывает новые возможности для подрывных действий. Стремительное расширение масштабов использования устройств мобильной связи, сетевых услуг, социальных сетей и услуг по обработке данных в удаленной среде расширяет круг проблем в сфере безопасности.

10. В условиях глобальной взаимосвязанности нашего мира неравенство возможностей государств в плане обеспечения безопасности ИКТ ведет к усилению уязвимости. Злоумышленники используют в своих целях слабозащищенные сети вне зависимости от их местоположения. Эту уязвимость усугубляют различия в национальном законодательстве, нормативных положениях и практических методах обеспечения безопасности ИКТ.

II. Укрепление сотрудничества в целях создания мирной, безопасной, устойчивой и открытой информационной среды

11. Государства-члены неоднократно заявляли о необходимости совместных действий, направленных на ликвидацию угроз, обусловленных злонамеренным использованием ИКТ. Чтобы добиться новых успехов в деле развития сотрудничества на международном уровне, необходимо осуществить комплекс мер, направленных на создание мирной, безопасной, открытой и основанной на сотрудничестве информационной среды. Необходимо рассмотреть совместные меры по укреплению международного мира, стабильности и безопасности. Такие меры включают выработку общего понимания в отношении применения соответствующих норм международного права и вытекающих из них норм, правил и принципов ответственного поведения государств.

12. Государства должны играть лидирующую роль в решении указанных вопросов, вместе с тем активное участие частного сектора и гражданского общества могло бы способствовать повышению эффективности сотрудничества.

13. Организация Объединенных Наций должна играть ведущую роль в поощрении диалога между государствами-членами для выработки общего понимания в отношении безопасности при использовании ИКТ и самих ИКТ, поощрять региональные усилия, меры по укреплению доверия и повышению транспарентности, а также способствовать наращиванию потенциала и распространению передового опыта.

14. В дополнение к работе, проводимой в рамках системы Организации Объединенных Наций, ценные усилия прилагают такие международные организации и региональные структуры, как Африканский союз, Региональный форум Ассоциации государств Юго-Восточной Азии (АСЕАН), Азиатско-Тихоокеанский форум экономического сотрудничества, Совет Европы, Экономическое сообщество западноафриканских государств (ЭКОВАС), Европейский союз, Лига арабских государств, Организация американских государств (ОАГ), Организация по безопасности и сотрудничеству в Европе (ОБСЕ) и Шанхайская организация сотрудничества. В будущем работа по вопросам безопасности в сфере использовании ИКТ должна вестись с учетом этих усилий.

15. Признавая всеобъемлющий характер данной проблемы, учитывая существующие и потенциальные угрозы, риски и факторы уязвимости и руководствуясь оценками и рекомендациями, содержащимися в опубликованном в июле 2010 года докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/65/201), Группа рекомендует следующие меры.

III. Рекомендации в отношении норм, правил и принципов ответственного поведения государств

16. Применение норм, основанных на положениях международного права, в отношении деятельности государств, связанной с использованием ИКТ, — необходимая предпосылка для снижения риска нарушения международного мира, безопасности и стабильности. Необходимо продолжать исследования для вы-

работки общего понимания того, как эти нормы применяются к поведению государств и использованию государствами ИКТ. С учетом уникальных особенностей ИКТ со временем могут быть разработаны дополнительные нормы.

17. Группа рассмотрела мнения и оценки государств-членов относительно достижений в сфере информатизации и телекоммуникаций в контексте международной безопасности, которые были представлены по просьбе Генеральной Ассамблеи, изложенной в ее резолюциях 64/25, 65/41 и 66/24, а также другие меры, предусмотренные в резолюциях 55/63, 56/121, 57/239, 58/199 и 64/211.

18. Группа отметила документ A/66/359, распространенный Генеральным секретарем по просьбе постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана и содержащий проект правил поведения в области обеспечения международной информационной безопасности, , к числу авторов которого впоследствии присоединились Казахстан и Кыргызстан.

19. Международное право, и в частности Устав Организации Объединенных Наций, применимо и имеет важное значение для поддержания мира и стабильности и создания открытой, безопасной, мирной и доступной информационной среды.

20. Государственный суверенитет и международные нормы и принципы, вытекающие из принципа государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием ИКТ, а также на юрисдикцию государств над ИКТ-инфраструктурой на их территории.

21. Предпринимаемые государством усилия по обеспечению безопасности ИКТ должны гармонично сочетаться с уважением прав человека и основных свобод, закрепленных во Всеобщей декларации прав человека и других международных инструментах.

22. Государства должны активизировать сотрудничество в борьбе с использованием ИКТ в преступных или террористических целях, надлежащим образом согласовывать свои правовые подходы и развивать практическое сотрудничество между соответствующими правоохранительными органами и органами прокуратуры.

23. Государства должны выполнять свои международные обязательства в отношении приписываемых им международно противоправных деяний. Государства не должны использовать посредников для совершения международно противоправных деяний. Государства должны стремиться не допускать того, чтобы негосударственные субъекты использовали их территорию для применения ИКТ в незаконных целях.

24. Государствам следует содействовать тому, чтобы частный сектор и гражданское общество играли надлежащую роль в укреплении безопасности при использовании ИКТ и самих ИКТ, включая безопасность всей системы производства и сбыта информационных товаров и информационно-технических услуг.

25. Государствам-членам следует изыскивать оптимальные формы сотрудничества в области осуществления вышеупомянутых норм и принципов ответственного поведения с учетом потенциальной роли частного сектора и организаций гражданского общества. Эти нормы и принципы дополняют усилия Организации Объединенных Наций и региональных групп и служат основой для дальнейшей работы по укреплению доверия и взаимопонимания.

IV. Рекомендации в отношении мер укрепления доверия и обмена информацией

26. Добровольные меры укрепления доверия могут способствовать установлению доверительных отношений между государствами и повышению степени доверия, а также уменьшают риск возникновения конфликтов благодаря обеспечению большей предсказуемости и снижению вероятности возникновения недопонимания. Они могут внести ценный вклад в решение вызывающих озабоченность государств проблем в связи с использованием ИКТ и стать важным шагом на пути к укреплению международной безопасности. Государствам следует рассмотреть вопрос о разработке, в частности, следующих практических мер по укреплению доверия для повышения транспарентности, обеспечения большей предсказуемости и развития сотрудничества:

a) добровольный обмен мнениями и информацией о национальных стратегиях и политике, передовом опыте, процессах принятия решений, соответствующих национальных организациях и мерах, направленных на развитие международного сотрудничества. Степень подробности такой информации будет определяться предоставляющими государствами. Обмен такой информацией может осуществляться на двусторонней основе, в рамках региональных групп или на других международных форумах;

b) создание двусторонних, региональных и многосторонних консультативных рамок для укрепления доверия, в частности проведение практикумов, семинаров и других учебных мероприятий, в целях содействия рассмотрению на национальном уровне вопросов о том, каким образом можно предотвратить деструктивные инциденты с использованием ИКТ, каким образом эти инциденты могут возникать и как им можно противодействовать;

c) улучшение обмена информацией между государствами об инцидентах, связанных с безопасностью ИКТ, посредством более эффективного использования существующих каналов или создания соответствующих новых каналов и механизмов для получения, сбора, анализа и распространения информации об инцидентах, связанных с использованием ИКТ, для своевременного реагирования на такие инциденты и осуществления мероприятий по устранению и смягчению последствий. Государствам следует рассмотреть возможность обмена информацией о национальных контактных центрах для расширения и улучшения существующих каналов связи, предназначенных для использования в целях управления в кризисных ситуациях, а также рассмотреть возможность оказания содействия усилиям по созданию или укреплению механизмов раннего предупреждения;

d) двусторонний обмен информацией и налаживание взаимодействия между национальными группами экстренной готовности к компьютерным ин-

цидентам, а также в рамках объединений таких групп и на других форумах в целях поддержания диалога на политическом и стратегическом уровнях;

e) расширение сотрудничества в деле противодействия инцидентам, которые могут затронуть инфраструктуру ИКТ или объекты критической инфраструктуры, где используются системы управления производственными процессами на основе ИКТ. Сюда могут входить разработка руководящих принципов и налаживание обмена передовым опытом между государствами по противодействию злонамеренным действиям, совершаемым негосударственными субъектами;

f) совершенствование механизмов сотрудничества правоохранительных органов для сокращения числа инцидентов, которые могли бы быть неверно истолкованы как враждебные действия со стороны государств, в целях укрепления международной безопасности.

27. Эти первоначальные меры укрепления доверия, позволяющие приобрести практический опыт, могут стать важным ориентиром для определения направлений будущей работы. Государствам следует содействовать закреплению и развитию прогресса, достигнутого на двустороннем и многостороннем уровнях, в том числе в рамках таких региональных групп, как Африканский союз, Региональный форум АСЕАН, Европейский союз, Лига арабских государств, Организация американских государств, ОБСЕ, Шанхайская организация сотрудничества и др. Опираясь на результаты этих усилий, государства должны содействовать обеспечению взаимодополняемости мер и распространению передового опыта с учетом специфики конкретных стран и регионов.

28. Государства должны играть лидирующую роль в разработке мер укрепления доверия, вместе с тем активное участие частного сектора и гражданского общества могло бы способствовать повышению эффективности таких усилий.

29. Учитывая темпы развития ИКТ и масштабы угрозы, Группа считает, что необходимо способствовать углублению общего понимания и активизации практического сотрудничества. В этой связи она рекомендует поддерживать регулярный институциональный диалог с широким кругом участников под эгидой Организации Объединенных Наций, а также регулярный диалог в рамках двусторонних, региональных и многосторонних форумов и других международных организаций.

V. Рекомендации в отношении мер по наращиванию потенциала

30. Решающим фактором повышения эффективности глобальных совместных усилий по обеспечению безопасности при использовании ИКТ и самих ИКТ является наращивание потенциала. Некоторым государствам может потребоваться помощь в связи с их усилиями по укреплению безопасности критически важной инфраструктуры ИКТ, развитию технических навыков и разработке соответствующего законодательства, стратегий и нормативно-правовой базы для того, чтобы они могли выполнить свои обязанности, а также преодолеть разрыв в уровне потенциала в области безопасности при использовании ИКТ и самих ИКТ.

31. В этой связи государствам, сотрудничающим с международными организациями, в том числе с учреждениями Организацией Объединенных Наций, и частному сектору следует рассмотреть наиболее эффективные способы оказания технической и иной помощи в целях наращивания потенциала в области безопасности при использовании ИКТ и самих ИКТ тем странам, который нуждаются в такой помощи, в особенности развивающимся государствам.

32. Опираясь на результаты работы по осуществлению ранее принятых резолюций, в частности резолюции 64/211, и положений ранее опубликованных докладов Организации Объединенных Наций по вопросам наращивания потенциала, государства должны рассмотреть возможность принятия следующих мер:

a) оказание поддержки двусторонним, региональным, многосторонним и международным мерам по наращиванию потенциала в целях обеспечения безопасного использования ИКТ и обеспечения безопасности ИКТ-инфраструктуры; развитие национальной правовой базы, укрепление потенциала правоохранительных органов и обеспечение эффективного осуществления принятых стратегий; борьба с использованием ИКТ в преступных и террористических целях; а также оказание помощи в выявлении и распространении передового опыта;

b) создание и укрепление потенциала реагирования на инциденты, в том числе групп экстренной готовности к компьютерным инцидентам, а также налаживание более тесного сотрудничества между такими группами;

c) содействие развитию и использованию электронных средств обучения, профессиональная подготовка и повышение осведомленности в вопросах безопасности ИКТ для преодоления «цифрового разрыва» и оказания развивающимся странам помощи, необходимой для непрерывного получения информации об изменениях международной стратегии;

d) расширение сотрудничества и передача знаний и технологий для предупреждения инцидентов, касающихся безопасности ИКТ, и ликвидации их последствий, особенно в интересах развивающихся стран;

e) оказание содействия научно-исследовательским институтам и университетам, с тем чтобы они продолжали работать над проблемами обеспечения безопасности ИКТ. С учетом возложенных на такие учреждения конкретных задач по оказанию поддержки государствам-членам и международному сообществу государствам следует рассмотреть вопрос о том, каким образом соответствующие научно-исследовательские и учебные институты Организации Объединенных Наций могли бы внести свой вклад в этом отношении.

33. Группа признала, что прогресс в отношении обеспечения безопасности использования ИКТ, в частности за счет поддержки усилий по созданию потенциала, будет также способствовать достижению восьмой цели в области развития, сформулированной в Декларации тысячелетия («Формирование глобального партнерства в целях развития»).

VI. Заключение

34. Прогресс в области обеспечения международной безопасности при использовании государствами ИКТ будет носить итеративный характер: каждый шаг основывается на уже достигнутых результатах. Необходимость такого подхода диктуется тем, что развитие технологического пространства происходит под воздействием постоянных изменений и неуклонного увеличения численности пользователей ИКТ. В настоящем докладе содержатся рекомендации, которые основываются на результатах ранее проделанной работы. Их осуществление и доработка будут способствовать укреплению доверия между всеми участниками. Группа рекомендует государствам-членам внимательно изучить настоящий доклад и подумать над возможными путями доработки и осуществления этих рекомендаций.

Приложение

Список членов Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

Аргентина
Посол Альфредо Морелли
Координатор, Отдел энергетики и технологий Министерства иностранных дел и по делам культов, Буэнос-Айрес

Австралия
Г-жа Дебора Стоукс
Первый помощник секретаря, Министерство иностранных дел и торговли, Канберра

Беларусь
Г-н Владимир Н. Герасимович
Начальник Управления международной безопасности и контроля над вооружениями Министерства иностранных дел, Минск

Канада
Г-н Майкл Валма
Директор Отдела политического планирования Министерства иностранных дел и международной торговли, Оттава

Китай
Г-н Лэй Ван (на первой и второй сессиях)
Директор Департамента контроля над вооружениями и разоружения Министерства иностранных дел, Пекин

Г-жа Чжихуа Дун (на третьей сессии)
Советник Департамента контроля над вооружениями и разоружения Министерства иностранных дел, Пекин

Египет
Д-р Шериф Хашим
Старший советник по кибербезопасности при Министре коммуникаций и информационных технологий, Министерство коммуникаций и информационных технологий, Каир

Эстония
Г-н Линнар Вик
Исполняющий обязанности директора Эстонского информационно-технологического колледжа, Таллинн

Франция
Г-н Жан-Франсуа Бларель
Заместитель генерального секретаря, координатор по вопросам киберпространства, Министерство иностранных дел, Париж

Германия
Г-н Детлеф Вольтер
Начальник Управления контроля над обычными вооружениями и по вопросам мер доверия и укрепления безопасности Федерального министерства иностранных дел, Берлин

Индия
Г-н Харш К. Джайн
Общий секретарь и руководитель Отдела электронного управления и информационных технологий Министерства иностранных дел, Нью-Дели

Индонезия
Г-н Фебриан Руддьярд (на первой сессии)
Директор по вопросам международной безопасности и разоружения, Министерство иностранных дел, Джакарта

Г-н Анди Рахмианто (на третьей сессии)
Советник-посланник, Постоянное представительство Индонезии при Организации Объединенных Наций, Нью-Йорк

Япония
Посол Тамоцу Шиноцука (на первой сессии)
Отдел международного сотрудничества в борьбе с терроризмом и международной организованной преступностью и по вопросам киберполитики, Министерство иностранных дел, Токио

Посол Осаму Имаи (на второй и третьей сессиях)
Отдел международного сотрудничества в борьбе с терроризмом и международной организованной преступностью и по вопросам киберполитики, Министерство иностранных дел, Токио

Российская Федерация
Г-н Андрей В. Крутских
Специальный координатор по вопросам политического использования ИКТ, Посол по особым поручениям, Министерство иностранных дел, Москва

Соединенное Королевство Великобритании и Северной Ирландии
Г-н Николас Хейкок
Помощник директора по международной безопасности, Управление кибербезопасности и обеспечения сохранности информации, секретариат Кабинета министров, Лондон

Соединенные Штаты Америки
Г-жа Мишель Маркофф
Заместитель координатора по вопросам киберпространства, Канцелярия Государственного секретаря, государственный департамент Соединенных Штатов Америки, Вашингтон, округ Колумбия