Организация Объединенных Наций A/C.2/64/L.8/Rev.1

# Генеральная Ассамблея

Distr.: Limited
20 November 2009
Russian
Original: English

**Шестьдесят четвертая сессия**
**Второй комитет**
Пункт 55(c) повестки дня
**Глобализация и взаимозависимость: наука и техника в целях развития**

**Австралия, Болгария, Венгрия, Израиль, Ирландия, Канада, Маршалловы Острова, Нигерия, Панама, Польша, Португалия, Республика Корея, Республика Молдова, Словения, Соединенное Королевство Великобритании и Северной Ирландии, Соединенные Штаты Америки, Франция, Эстония и Япония: проект резолюции**

## Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур

*Генеральная Ассамблея*,

*ссылаясь* на свои резолюции 55/63 от 4 декабря 2000 года и 56/121 от 19 декабря 2001 года о борьбе с преступным использованием информационных технологий, 57/239 от 20 декабря 2002 года о создании глобальной культуры кибербезопасности и 58/199 от 23 декабря 2003 года о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур,

*ссылаясь также* на свои резолюции 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 и 63/37 от 2 декабря 2008 года о достижениях в области информационных технологий в контексте международной безопасности,

*ссылаясь далее* на итоговые документы Всемирной встречи на высшем уровне по вопросам информационного общества, состоявшейся в 2003 году (первый этап) и в 2005 году (второй этап)[1], ,

[1] См. A/C.2/59/3 и A/60/687.

*признавая*, что доверие и безопасность в использовании информационно-коммуникационных технологий относятся к главным опорам информационного общества и что необходимо поощрять, формировать, развивать и активно внедрять устойчивую глобальную культуру кибербезопасности,

*признавая также* растущий вклад сетевых информационных технологий в выполнение многих важнейших функций в повседневной жизни, торговлю и обеспечение товарами и услугами, научные исследования, инновационную деятельность, предпринимательство и свободную передачу информации между физическими лицами и организациями, правительствами, деловыми кругами и гражданским обществом;

*признавая далее*, что правительства, деловые круги, другие организации и индивидуальные владельцы и пользователи информационных технологий должны нести ответственность, сообразную их функциям, за обеспечение безопасности этих информационных технологий и принимать надлежащие меры для ее укрепления,

*признавая* важность мандата Форума по вопросам управления Интернетом как площадки для диалога между многими заинтересованными сторонами для обсуждения различных вопросов, включая, в частности, вопросы государственной политики в связи с ключевыми элементами управления Интернетом, для содействия обеспечению устойчивого характера, надежности, безопасности, стабильности и развития Интернета и вновь заявляя о том, что все правительства должны иметь равные задачи и обязанности в сфере управления Интернетом на международной основе и обеспечения стабильности, безопасности и непрерывности Интернета,

*вновь подтверждая* сохраняющуюся необходимость упрочения сотрудничества — с тем чтобы правительства могли на равной основе играть свою роль и выполнять свои обязательства — в решении вопросов международной государственной политики, касающихся Интернета, а не в сфере повседневной деятельности технического и эксплуатационного характера, которые не влияют на вопросы международной государственной политики,

*признавая*, что каждая страна будет сама определять свои собственные важнейшие информационные инфраструктуры,

*вновь подтверждая* необходимость использования потенциала информационно-коммуникационных технологий для содействия достижению согласованных на международном уровне целей в области развития, в том числе сформулированных в Декларации тысячелетия, и признавая, что отсутствие равного доступа к информационным технологиям и возможностей их использования государствами может подорвать их экономическое процветание и эффективность сотрудничества в борьбе с преступным использованием информационных технологий и в создании глобальной культуры кибербезопасности,

*подчеркивая* необходимость активизации усилий по преодолению «цифровой пропасти» для обеспечения универсального доступа к информационно-коммуникационным технологиям и для защиты важнейших информационных инфраструктур путем облегчения передачи информационных технологий развивающимся странам, особенно наименее развитым странам, и наращивания их потенциала в вопросах передовой практики и профессиональной подготовки в области кибербезопасности,

*выражая озабоченность* по поводу того, что угрозы надежному функционированию важнейших информационных инфраструктур и целостности информации, передаваемой по этим сетям, приобретают все более изощренный и серьезный характер, отрицательно сказываясь на уровне семейного, национального и международного благополучия,

*подтверждая*, что обеспечение защищенности важнейших информационных инфраструктур — это обязанность, которую правительства должны систематически выполнять, выступая с соответствующими инициативами на национальном уровне, в координации с заинтересованными сторонами, которые, в свою очередь, должны знать о соответствующих рисках, превентивных мерах и эффективных мерах реагирования, соответствующих возложенным на них функциям,

*признавая*, что национальные усилия должны подкрепляться обменом информацией и взаимодействием на международном уровне, с тем чтобы можно было эффективно противостоять таким угрозам, приобретающим все более транснациональный характер,

*отмечая* работу соответствующих региональных и международных организаций по укреплению кибербезопасности и вновь указывая на их роль в поддержании национальных усилий и поощрении международного сотрудничества,

*отмечая также* подготовленный Международным союзом электросвязи в 2009 году доклад “Securing information and communication networks: best practices for developing a culture of cybersecurity” («Обеспечение защищенности информационно-коммуникационных сетей: передовая практика в области формирования культуры кибербезопасности»), основное внимание в котором уделяется всеобъемлющему национальному подходу к кибербезопасности, не нарушающему свободы слова, свободы передачи информации и надлежащих правовых процедур,

*признавая*, что национальные усилия по защите важнейших информационных инфраструктур выигрывают от периодической оценки их прогресса,

1. *предлагает* государствам-членам использовать, если и когда они сочтут это целесообразным, прилагаемый инструмент добровольной самооценки национальных усилий по защите важнейших информационных инфраструктур, призванный помочь им в анализе их усилий по защите важнейших информационных инфраструктур и укреплению кибербезопасности, с тем чтобы выявить области, в которых требуется принятие дополнительных мер, в целях повышения глобальной культуры кибербезопасности;

2. *рекомендует* государствам-членам и соответствующим региональным и международным организациям, разработавшим стратегии действий в области кибербезопасности и защиты важнейших информационных инфраструктур, поделиться сведениями о передовой практике и мерах, которые могли бы помочь другим государствам-членам в их усилиях по содействию обеспечению кибербезопасности, путем представления такой информации Генеральному секретарю для ее обобщения и распространения среди государств-членов.

## Приложение

### Инструмент добровольной самооценки национальных усилий по защите важнейших информационных [a]

*Анализ потребностей и стратегий в области кибербезопасности*

1. Проанализируйте роль информационно-коммуникационных технологий в Вашей национальной экономике, национальной безопасности, важнейших инфраструктурах (таких как транспорт, водоснабжение и обеспечение продовольствием, общественное здравоохранение, энергетика, финансы, службы экстренной помощи) и гражданском обществе.

2. Определите риски в области кибербезопасности и защиты важнейших информационных инфраструктур для экономики, национальной безопасности, важнейших инфраструктур и гражданского общества Вашей страны, которые нуждаются в управлении.

3. Выявите слабые места в используемых сетях, относительные уровни текущих угроз в каждом секторе и существующий план управления; обратите внимание, как на этих расчетах сказываются изменения в экономической ситуации, приоритетах в области национальной безопасности и потребностях гражданского общества.

4. Определите цели национальной стратегии по обеспечению кибербезопасности и защиты важнейших информационных инфраструктур, опишите эти цели, нынешний уровень достижения, существующие меры по оценке достигнутого прогресса, связь стратегии с задачами национальной политики, а также, как эта стратегия вписывается в региональные и международные инициативы.

*Роли и обязанности заинтересованных сторон*

5. Определите ключевые заинтересованные стороны, участвующие в обеспечении кибербезопасности и защиты важнейших информационных инфраструктур, и опишите роль каждой из них в разработке соответствующих стратегий и операций, включая:

- национальные государственные министерства и ведомства с указанием главных лиц для контактов и обязанностей каждого из них;
- других государственных (местных и региональных) участников;
- неправительственных участников, включая представителей промышленности, гражданского общества и научных кругов;
- отдельных граждан с указанием того, имеют ли рядовые пользователи Интернета доступ к базовой подготовке, позволяющей избегать угроз в Интернете, и проводится ли национальная кампания распространения информации по вопросу кибербезопасности.

---

[a] Это добровольный инструмент, который может использоваться государствами-членами (полностью или частично, если и когда они сочтут это целесообразным) и который призван помочь им в анализе их усилий по защите важнейших информационных инфраструктур и укреплению кибербезопасности.

*Стратегические процессы и участие*

6. Перечислите существующие в настоящее время формальные и неформальные механизмы взаимодействия между правительством и промышленностью в разработке стратегий и операций в области кибербезопасности и защиты важнейших информационных инфраструктур; определите участников, роль(и) и задачи, методы мобилизации и анализа вклада в эту деятельность и то, насколько он обеспечивает достижение соответствующих целей в области кибербезопасности и защиты важнейших информационных инфраструктур.

7. Определите форумы или структуры, которые могут в дальнейшем понадобиться для интеграции позиций правительства и неправительственных участников и их знаний, что необходимо для достижения национальных целей в области кибербезопасности и защиты важнейших информационных инфраструктур.

*Сотрудничество между государственным и частным секторами*

8. Представьте сводную информацию о всех принятых мерах и планах по развитию сотрудничества между правительством и частным сектором, включая любые механизмы распространения информации и реагирования на инциденты.

9. Представьте сводную информацию о всех осуществляемых и запланированных инициативах по отстаиванию общих интересов и решению общих проблем как среди участников важнейших инфраструктур, так и среди представителей частного сектора, в равной степени зависящих от пользования одними и теми же взаимосвязанными важнейшими инфраструктурами.

*Деятельность в связи с инцидентами и восстановление после сбоев*

10. Укажите государственное ведомство, выполняющее функции координатора деятельности в связи с инцидентами, включая возможные функции наблюдения, предупреждения, реагирования и восстановления; сотрудничающие с ним государственные ведомства; сотрудничающих неправительственных участников, включая представителей промышленности и других партнеров; и любые существующие механизмы сотрудничества и обмена достоверной информацией.

11. Отдельно укажите общенациональный механизм реагирования на компьютерные сбои, включая любую группу реагирования на компьютерные сбои, выполняющую общенациональные функции, и перечислите ее функции и обязанности, в том числе опишите существующий инструментарий и процедуры защиты правительственных компьютерных сетей и существующие инструменты и процедуры распространения информации о деятельности в связи с инцидентами.

12. Укажите сети и процессы международного сотрудничества, которые могут укрепить потенциал реагирования на инциденты и планирования на случай чрезвычайных ситуаций, отдельно выделив в соответствующих случаях партнеров и механизмы двустороннего и многостороннего сотрудничества.

*Правовые рамки*

13. Проанализируйте и обновите список национальных правовых органов (в том числе занимающихся вопросами киберпреступности, охраны личной информации, защиты данных, коммерческого права, цифровых подписей и шифрования), которые могут устареть или утратить актуальность в результате быстрого развития новых информационно-коммуникационных технологий и формирования зависимости от них, используя в ходе этого рассмотрения региональные и международные конвенции, механизмы и прецеденты. Установите, разработала ли Ваша страна необходимое законодательство для расследования киберпреступлений и преследования лиц, виновных в их совершении, обратив внимание на существующие механизмы, например на резолюции 55/63 и 56/121 Генеральной Ассамблеи Организации Объединенных Наций о борьбе с преступным использованием информационных технологий и на региональные инициативы, включая Конвенцию Совета Европы о киберпреступности.

14. Определите нынешнее состояние национальных органов по борьбе с киберпреступностью и соответствующих процедур, включая правовые органы, национальные группы по борьбе с киберпреступностью, и уровень взаимопонимания между прокурорами, судьями и законодателями, занимающимися вопросами киберпреступности.

15. Оцените, насколько существующие правовые кодексы и правовые органы соответствуют задаче решения существующих и будущих проблем киберпреступности и киберпространства в целом.

16. Изучите уровень национального участия в международной деятельности по борьбе с киберпреступностью, такой как функционирующая круглосуточно без выходных Сеть контактных пунктов по киберпреступности.

17. Определите потребности национальных правоохранительных органов в сотрудничестве с международными коллегами при расследовании транснациональных киберпреступлений в тех случаях, когда инфраструктура или лица, обвиняемые в совершении этих преступлений, находятся на Вашей национальной территории, а жертва находится за пределами Вашей страны.

*Формирование глобальной культуры кибербезопасности*

18. Представьте сводную информацию о принятых мерах и планах по формированию национальной культуры кибербезопасности, о которой говорится в резолюциях 57/239 и 58/199 Генеральной Ассамблеи Организации Объединенных Наций, включая реализацию плана кибербезопасности для систем, управление которыми осуществляет правительство, национальных программ повышения уровня осведомленности и распространения знаний среди, в частности, детей и индивидуальных пользователей, а также о потребностях в профессиональной подготовке в области национальной кибербезопасности и защиты важнейших информационных инфраструктур.