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

Генеральная Ассамблея

Distr.: Limited
22 October 2009
Russian
Original: English

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

Австралия, Израиль, Канада, Маршалловы Острова, Соединенные Штаты Америки 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 сфере информатизации и телекоммуникаций в контексте международной безопасности,

ссылаясь далее на итоговые документы Всемирной встречи на высшем уровне по вопросам информационного общества, состоявшейся 10–12 декабря 2003 года в Женеве (первый этап) и 16–18 ноября 2005 года в Тунисе (второй этап)[1], в которых государства признали, что свобода выражения мнений и свободный поток информации, идей и знаний имеют существенное значение для информационного общества и благоприятствуют развитию и что, поскольку доверие и безопасность относятся к главным опорам информационного обще-

[1] См. A/C.2/59/3 и A/60/687.

ства, необходимо поощрять, формировать, развивать и активно внедрять устойчивую глобальную культуру кибербезопасности,

признавая все более незаменимый вклад сетевых информационных технологий в выполнение большинства важнейших функций в повседневной жизни, торговлю и обеспечение товарами и услугами, научные исследования, инновационную деятельность и предпринимательство и свободную передачу информации между физическими лицами, организациями и правительствами;

отмечая, что правительства, деловые круги, гражданское общество и физические лица все более зависят от глобальной сети информационных инфраструктур и что такая зависимость будет лишь возрастать,

отмечая также, что отсутствие равного доступа к информационным технологиям и возможностей их использования государствами может подорвать их социально-экономическое процветание, и особо отмечая потребности менее развитых стран в передовых практических методах и профессиональной подготовке в вопросах кибербезопасности,

выражая обеспокоенность 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 национальном, региональном и международном уровнях, с тем чтобы можно было эффективно противостоять таким угрозам, приобретающим все более транснациональный характер,

отмечая работу соответствующих региональных и международных организаций по укреплению кибербезопасности, особенно тех из них, которые поддерживают национальные усилия и поощряют международное сотрудничество,

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 создания культуры кибербезопасности»), основное внимание в котором уделяется всеобъемлющему национальному подходу к кибербезопасности, не нарушающему свободу слова, свободу 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 на добровольной основе представлять краткую информацию об их ключевых инициативах в области кибербезопасности и защиты важнейших информационных инфраструктур, с тем чтобы выделить национальные достижения и передовую практику, извлеченные уроки и направления будущей деятельности;

2. *предлагает* в этой связи вниманию государств-членов прилагаемый национальный вопросник для самооценки усилий в области кибербезопасности в качестве одного из возможных инструментов для оказания им, в соответствующих случаях, содействия в оценке национальных усилий в области кибербезопасности и защиты важнейших информационных инфраструктур;

3. *предлагает* всем государствам-членам, разработавшим стратегии действий в области кибербезопасности и защиты важнейших информационных инфраструктур, информировать Генерального секретаря к шестьдесят пятой сессии Генеральной Ассамблеи о передовой практике и мерах, которые могли бы помочь другим государствам-членам, региональным и международным организациям, заинтересованным лицам в частном секторе и в гражданском обществе в их усилиях по созданию глобальной культуры кибербезопасности.

Приложение

Инструмент самооценки национальных усилий по защите важнейших информационных инфраструктур

Анализ потребностей и стратегий в области кибербезопасности

1. Оцените 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 вашей экономики, национальной безопасности, важнейших инфраструктур и гражданского общества, которые нуждаются в регулировании.

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

4. Определите цели вашей национальной стратегии по обеспечению кибербезопасности и защиты важнейших информационных инфраструктур, опишите эти цели, нынешний уровень достижения, существующие меры по оценке хода их достижения, их связь 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.

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 за-

щиты важнейших информационных инфраструктур; определите участников, роль(и) и задачи, методы мобилизации и анализа вклада в эту деятельность и 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 пользователей важнейших инфраструктур, так и среди представителей частного сектора, в равной степени зависящих от использования одних и тех же взаимосвязанных важнейших инфраструктур.

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 учреждения; 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. Определите, является ли ваше государство участником Будапештской конвенции о киберпреступности, планирует ли присоединиться к ней или же планирует принять сопоставимые законы.

14. Определите нынешнее состояние национальных органов по борьбе с киберпреступностью и соответствующих процедур, включая правовые органы и 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. Проанализируйте, участвует ли ваше государство в международной деятельности по борьбе с киберпреступностью, такой как функционирующая круглосуточно без выходных Сеть контактных пунктов по киберпреступности, и определите, в какой мере такое участие способствует достижению национальных целей в области кибербезопасности.

17. Установите для ваших национальных правоохранительных органов требование сотрудничать с международными коллегами в 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.

Создание глобальной культуры кибербезопасности

18. Представьте сводную информацию о принятых мерах и планах по созданию 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.