Организация Объединенных Наций A/62/98/Add.1

Генеральная Ассамблея

Distr.: General
17 September 2007
Russian
Original: English

Шестьдесят вторая сессия
Пункт 95 предварительной повестки дня*
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Доклад Генерального секретаря

Добавление

II. Ответы, полученные от правительств (*продолжение*)

Бангладеш

[Подлинный текст на английском языке]
[29 июня 2007 года]

Мир достиг значительного прогресса в разработке и внедрении новейших информационных технологий, что открывает широкие возможности для развития цивилизации на основе распространения информации в общемировом масштабе. Вместе с тем террористы или преступники могут использовать информационные технологии в целях, идущих вразрез с интересами обеспечения международной стабильности и безопасности, и поэтому необходимо предотвращать их использование преступниками или террористами. Исходя из этого Бангладеш одобряет принятие резолюции 61/54 Генеральной Ассамблеи.

* A/62/150.

07-50792 (R) 270907 270907

Бруней-Даруссалам

[Подлинный текст на английском языке]
[29 августа 2007 года]

[Нижеследующая информация была получена от правительства Брунея-Даруссалама в дополнение к информации, уже включенной в документ A/62/98.]

1. Ключевые моменты

Общая оценка вопросов информационной безопасности

1. Управление по информационно-коммуникационным технологиям (УИКТ) и министерство коммуникаций Брунея-Даруссалама высоко ценят проводимую Организацией Объединенных Наций работу по разъяснению важного значения информационной безопасности на международном уровне. Мы поддерживаем продолжающуюся международную дискуссию по этому вопросу, призванную стимулировать дальнейшее международное сотрудничество в этой области.

Принятые на национальном уровне меры по укреплению информационной безопасности и содействию международному сотрудничеству в этой сфере

2. С 2000 года в Брунее действует законодательство, предусматривающее уголовную ответственность за нарушение правил эксплуатации компьютерной техники и других соответствующих средств телекоммуникаций. Кроме того, в 2004 году нами была сформирована Национальная группа быстрого реагирования на угрозы безопасности вычислительных систем (БруСЕРТ), призванная координировать принимаемые на национальном уровне меры в связи с угрозами информационной безопасности и взаимодействовать на региональном уровне с Азиатско-тихоокеанской группой быстрого реагирования на угрозы безопасности вычислительных систем.

Возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне

3. По мнению УИКТ, создание на национальном, региональном и международном уровнях групп реагирования на угрозы безопасности вычислительных систем является адекватной ответной мерой на угрозы информационной безопасности. Методы, применяемые для подрыва систем преступными сообществами, столь же легко могут применяться и воюющими государствами, и террористическими организациями.

2. Общая оценка вопросов информационной безопасности

4. С учетом все более активного и повсеместного проникновения информационных технологий в гражданскую и военную области УИКТ сознает необходимость повышения осведомленности на национальном и международном уровнях об угрозах информационной безопасности.

3. Меры, принятые на национальном уровне

Законы, разработанные в 2000 году

5. Постановление о нарушении правил эксплуатации компьютерной техники (2000 год) дает описательное определение «нарушений» в сфере компьютерных технологий. Оно охватывает различные виды нарушений, касающихся не только Интернет-систем, но и сотовых телефонов и других телекоммуникационных устройств.

6. На момент подготовки настоящего доклада (май 2007 года) это законодательство еще не применялось для преследования по уголовным делам, связанным с нарушением правил эксплуатации компьютерной техники.

Брунейская национальная группа быстрого реагирования на угрозы безопасности вычислительных систем

7. БруСЕРТ была создана в мае 2004 года во взаимодействии с УИКТ и министерством коммуникаций в качестве первого специализированного учреждения страны, призванного решать весь спектр вопросов, связанных с происшествиями в сфере компьютерных технологий и Интернета в Брунее-Даруссаламе.

8. Это согласуется с обязательствами содействовать международному сотрудничеству, взятыми на уровне Рабочей группы Азиатско-тихоокеанского экономического сотрудничества по телекоммуникациям и информации (АТЭС-ТЕЛ).

9. БруСЕРТ взаимодействует с местными и международными группами реагирования на угрозы безопасности вычислительных систем, организациями, оказывающими сетевые услуги, поставщиками систем безопасности, государственными ведомствами и другими соответствующими организациями с целью содействия выявлению, анализу и предупреждению инцидентов, представляющих угрозу для Интернета.

4. Возможные меры по укреплению информационной безопасности

10. С учетом трансграничного характера действий, представляющих угрозу для информационных систем, УИКТ полагает, что существующая сеть групп реагирования на угрозы безопасности вычислительных систем является надлежащим механизмом для распространения информации и обмена знаниями в международном масштабе.

11. В отличие от «традиционных» методов ведения войны, подрыв национальной безопасности посредством вмешательства в информационные системы не требует производства или приобретения военных средств или оружия массового уничтожения. Следовательно, существующая сеть групп быстрого реагирования на угрозы безопасности вычислительных систем должна быть достаточной для противодействия согласованным мерам трансграничного характера по подрыву сетей.

12. В Брунее-Даруссаламе существующие механизмы международного преследования за уголовные преступления распространяются и на преступления, предусмотренные Постановлением о нарушении правил эксплуатации компьютерной техники 2000 года. В этой связи УИКТ подчеркивает, что международ-

ное сотрудничество имеет важное значение для преследования лиц, совершивших преступления в сфере информационной безопасности.