Полномочная конференция (ПК-06)
Анталия, 6–24 ноября 2006 г.

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

Документ 24-R
4 сентября 2006 года
Оригинал: английский

Записка Генерального секретаря

ОТЧЕТ О СОБРАНИИ ПО ВОПРОСУ МЕХАНИЗМОВ СОТРУДНИЧЕСТВА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ И БОРЬБЫ СО СПАМОМ (РЕЗОЛЮЦИЯ 45 (ВКРЭ-06)) (Женева, 31 августа – 1 сентября 2006 года)

1 Введение

ВКРЭ-06 приняла Резолюцию 45, в которой Директору БРЭ было поручено организовать собрание в соответствии с Программой 3 Дохинского плана действий по вопросу механизмов сотрудничества в области кибербезопасности и борьбы со спамом и представить отчет о результатах этого собрания Полномочной конференции МСЭ 2006 года.

Собрание открыл Директор БРЭ г-н Хамадун ТУРЕ, в своих вступительных замечаниях подчеркнувший значимость кибербезопасности, широкий круг связанных с ней вопросов и важность того, чтобы на собрании были приняты конкретные решения, направленные на удовлетворение потребностей всех членов Союза, учитывая особые проблемы, с которыми сталкиваются развивающиеся страны, а также имеющиеся решения таких проблем.

На собрании председательствовал г-н Махтар ФОЛЛ из Сенегала, которому помогал г-н Александр НТОКО из БРЭ. Председатель представил повестку дня, которая была принята. В своих вступительных замечаниях председатель выделил проблемы, с которыми сталкиваются развивающиеся страны в этой области, и призвал к духу сотрудничества и консенсусу, необходимым для достижения конкретных результатов.

На данном мероприятии, проходившем в течение двух дней, присутствовали около 50 делегатов от 24 Государств – Членов, Членов Секторов, Управления Организации Объединенных Наций по наркотикам и преступности, Совета Европы, Европейской комиссии, Всемирного банка и персонала МСЭ (БРЭ, БСЭ и Генерального секретариата). Собрание было организовано на шести (6) языках МСЭ. Дополнительная информация и справочные документы представлены по адресу: http://www.itu.int/ITU-D/cybersecurity.

2 Представление исходных документов

После принятия повестки дня и вступительных замечаний председателя БРЭ представило материалы, касающиеся мандата Сектора развития в области кибербезопасности и борьбы со спамом. В качестве источников обсуждений и идей были использованы и другие справочные и вспомогательные документы. Материалы, касающиеся национальных, региональных, многосторонних и международных инициатив в области кибербезопасности и борьбы со спамом были представлены Австралией, Cisco Systems, Советом Европы, Европейской комиссией, Литвой, Нигером, Российской Федерацией, Суданом, Сирийской Арабской Республикой от имени арабских государств, Соединенным Королевством, Соединенными Штатами Америки, Узбекистаном и Всемирным банком. Предложенные инициативы касались вопросов создания потенциала, законодательства, технологий, реагирования на происшествия, политики и стратегий, партнерств, а также механизмов правоприменения.

В дополнение к имеющимся инициативам делегаты из развивающихся стран представили новые, включая предложения о разработке Меморандума о взаимопонимании. Представленные вклады свидетельствовали о наличии нескольких инициатив, большинство из которых осуществляется развитыми странами при ограниченном участии развивающихся.

3 Обсуждения и анализ

Делегаты прокомментировали представленные материалы и выдвинули несколько предложений относительно возможного направления дальнейших действий. Важность сотрудничества и совместной работы подчеркивалась в большинстве выступлений и обсуждений. Делегаты согласились с необходимостью мобилизации имеющегося экспертного опыта в целях удовлетворения потребностей развивающихся стран. В ходе большинства выступлений и обсуждений были определены области, где, как представляется, существует необходимость в принятии мер на национальном, региональном и международном уровнях. В качестве направлений деятельности, важных для сотрудничества Государств-Членов в области кибербезопасности и борьбы со спамом, были определены такие области, как создание потенциала, национальное законодательство, национальная политика и стратегии, партнерства государственного/частного секторов, механизмы правоприменения, обмен информацией, назначение национальных координаторов, реагирование на происшествия и технологические решения. Участники пришли к общему пониманию необходимости внедрения некоторых механизмов для оказания содействия попросившим об этом странам. В ходе обсуждений и анализа задач[1] и осуществляемых инициатив было очевидно, что даже если в целом вопросы, связанные с угрозами в области кибербезопасности и спамом, необходимо решать на глобальном уровне, должны быть удовлетворены и конкретные потребности, в особенности потребности развивающихся стран. Для участия всех заинтересованных стран (развивающихся и развитых) в мире глобальных и многосторонних инициатив необходимо, чтобы все страны удовлетворяли некоторым минимальным национальным требованиям в таких областях, как законодательство, человеческий и организационный потенциал, а также соответствующие политика и стратегии.

В результате выступлений и обсуждений был определен ряд областей, в которых МСЭ-D следует предпринять дальнейшие действия для решения задач, с которыми сталкиваются развивающиеся и наименее развитые страны.

Было решено, что помимо того, что многие направления деятельности следует осуществлять на национальном уровне, имеется необходимость в сотрудничестве различных заинтересованных сторон и координации инициатив и что МСЭ-D в рамках своего мандата должен содействовать выполнению действий, в отношении которых поступили просьбы Государств-Членов. Было высказано мнение, что в этом контексте могут быть установлены определенные практические задачи, и при их решении следует использовать опыт и компетенцию МСЭ.

В соответствии со смыслом и целью Резолюции 45 и учитывая общее согласие в отношении того, что в некоторых областях деятельности требуется координация, выходящая за пределы существующих основ, далее основной задачей являлось принятие решения о типе механизма, с помощью которого МСЭ-D окажет необходимое содействие развивающимся странам. На обсуждение были представлены три варианта:

a) Меморандум о взаимопонимании между заинтересованными Государствами-Членами, депозитарием которого стал бы Генеральный секретарь МСЭ.

b) Основа для технического сотрудничества между МСЭ и заинтересованными Государствами-Членами и партнерами.

c) Проект по выполнению Резолюции 45 для заинтересованных сторон и при участии обладающих признанным опытом объединений.

---

[1] Пункт c) раздела *признавая* Резолюции 45 ВКРЭ-06 (Приложение 1).

Все три варианта направлены на внедрение механизмов совершенствования сотрудничества между заинтересованными сторонами при использовании опыта и знаний действующих объединений и осуществляемых инициатив. Все три варианта не будут носить обязательного характера для Государств-Членов, будут открыты для заинтересованных стран и направлены на удовлетворение потребностей стран, не охваченных существующими рамками сотрудничества.

Одним из важных принятых во внимание соображений было то, что в мандат МСЭ-D в области кибербезопасности и борьбы со спамом входят, в частности, три основных элемента – Программа 3 Дохинского плана действий, Вопрос 22 1-й Исследовательской комиссии МСЭ-D, а также Резолюция 45 ВКРЭ-06. Выводы и рекомендации, сделанные на собрании, таким образом, были направлены на разработку предложений, пока не являющихся частью решений, согласованных членами Союза на ВКРЭ-06. Такие предложения должны охватывать деятельность по разработке механизмов, не затрагиваемых в существующих решениях, однако необходимых развивающимся странам, от которых поступают соответствующие просьбы.

4 Рекомендации в отношении дальнейших действий

По итогам тематического собрания ВВУИО по противодействию спаму были определены следующие важные направления для работы в сфере кибербезопасности и борьбы со спамом.

1) Сильное законодательство.
2) Разработка технических мер.
3) Создание промышленных партнерств, особенно с поставщиками услуг интернета, операторами подвижной связи и ассоциациями по прямому маркетингу.
4) Осведомленность заказчиков и представителей отрасли о мерах противодействия спаму и примерах передового опыта в области безопасности интернета.
5) Международное сотрудничество на уровне правительств, отрасли, заказчиков, коммерческих предприятий и групп по противодействию спаму для обеспечения глобального и скоординированного подхода к данной проблеме.

В дополнение к перечисленному выше в ходе обсуждений и выступлений были также определены направления, представленные далее без разбивки по приоритетному значению, также являющиеся важными для сотрудничества и оказания содействия Государствам-Членам, которые МСЭ-D может осуществлять совместно с объединениями, обладающими признанным опытом в области кибербезопасности и борьбы со спамом:

a) Формирование общего представления о проблеме.
b) Соответствующее национальное законодательство.
c) Создание человеческого и организационного потенциала.
d) Правоприменительная деятельность (в сфере создания потенциала).
e) Национальная политика и стратегии в области кибербезопасности.
f) Обмен информацией между странами и соответствующими заинтересованными сторонами.
g) Назначение национальных координаторов.
h) Мониторинг и оценка хода выполнения существующих инициатив.
i) Реагирование на происшествия, наблюдение и предупреждение.
j) Оценка уязвимых мест и угроз в области кибербезопасности.
k) Эффективные инструменты и приложения для сети и кибербезопасности.
l) Партнерства.
m) Международное сотрудничество.

Собрание пришло к консенсусу в том, что МСЭ-D должен играть ключевую роль в объединении существующих инициатив и обеспечивать базу, объединяющую данные инициативы в целях удовлетворения потребностей развивающихся стран.

Собрание предложило МСЭ-D должным образом учесть соответствующую деятельность других заинтересованных сторон, обладающих признанным опытом в данной области. К ней относится деятельность по противодействию спаму, проводимая в рамках МСЭ-Т, Лондонского плана действий, Всемирного банка, Сеульско-Мельбурнского меморандума о взаимопонимании (МоВ), Управления Организации Объединенных Наций по наркотикам и преступности, Конвенции Совета Европы о борьбе с киберпреступностью, Рабочей группы по электросвязи и информации Организации азиатско-тихоокеанского экономического сотрудничества (АТЭС TEL), Организации экономического сотрудничества и развития (ОЭСР), а также другими соответствующими партнерами.

Для деятельности в вышеперечисленных областях собрание посчитало, что БРЭ в рамках координации Программы 3 должно разработать проект по механизму выполнения Резолюции 45 ВКРЭ-06. Основываясь на потребностях и приоритетах развивающихся стран, нуждающихся в содействии МСЭ в данной области, в проекте следует должным образом учитывать признанный опыт действующих в данной области объединений и осуществляемые инициативы, включая деятельность по противодействию спаму, проводимую в рамках МСЭ-Т, Лондонского плана действий, Всемирного банка, Сеульско-Мельбурнского меморандума о взаимопонимании (МоВ), Управления Организации Объединенных Наций по наркотикам и преступности, Конвенции о киберпреступности Совета Европы, Рабочей группы по электросвязи и информации Организации азиатско-тихоокеанского экономического сотрудничества (АТЭС TEL), Организации экономического сотрудничества и развития (ОЭСР), а также другими соответствующими партнерами, но не ограничиваясь этим.

Информация по проекту:

- Проект под названием "Проект по расширению сотрудничества в области кибербезопасности и борьбы со спамом" будет длиться 4 года начиная с 2007 года и являться частью оперативного плана БРЭ на 2007 год.
- На сессиях Совета МСЭ будут предоставляться ежегодные отчеты о ходе деятельности по его выполнению.
- При выполнении проекта следует учитывать решения ВКРЭ-06, касающиеся мандата Сектора развития в области кибербезопасности и борьбы со спамом.
- Проект должен быть в первую очередь направлен на оказание содействия развивающимся странам в вышеуказанных областях путем налаживания жизненно важного сотрудничества в области кибербезопасности и борьбы со спамом.
- В отношении соответствующего законодательства следует должным образом учитывать работу в данной области Совета Европы по оказанию содействия странам в разработке национального законодательства, соответствующего положениям Конвенции о борьбе с киберпреступностью.
- Осуществление деятельности в рамках данного проекта должно основываться на поступивших от стран просьбах, особое внимание уделяя развивающимся странам.
- После разработки проект должен быть представлен потенциальным финансирующим объединениям, включая Государства-Члены, частный сектор и международные организации, такие как Всемирный банк и Европейская комиссия.

ПРИЛОЖЕНИЕ

РЕЗОЛЮЦИЯ 45 (Доха, 2006 г.)

Механизмы совершенствования сотрудничества в области кибербезопасности, включая борьбу со спамом

Всемирная конференция по развитию электросвязи (Доха, 2006 г.),

напоминая

a) благородные принципы, цели и задачи, включенные в Устав Организации Объединенных Наций и во Всеобщую декларацию прав человека;

b) предоставляемую ею существенную поддержку Программе 3 (Электронные стратегии и приложения на базе ИКТ), подтверждая, что в рамках этой программы будут выполняться основные задачи по Направлению деятельности С5 Тунисской программы "Укрепление доверия и безопасности при использовании ИКТ";

c) положения пунктов 35, 36 и 37 Женевской декларации принципов;

d) положения пункта 15 Тунисского обязательства,

учитывая

a) роль информационно-коммуникационных технологий (ИКТ) как эффективных инструментов содействия делу мира, безопасности и стабильности, укрепления демократии, социальной сплоченности, надлежащего управления и верховенства права, а также необходимость противодействовать вызовам и угрозам, возникающим в результате злоупотребления этими технологиями, в том числе в преступных и террористических целях, обеспечивая при этом соблюдение прав человека (пункт 15 Тунисского обязательства);

b) необходимость обеспечения доверия и безопасности при использовании ИКТ (пункт 39 Тунисской программы) и уголовного преследования киберпреступности на национальном и региональном уровнях, учитывая существующие нормативные базы, например резолюции 55/63 и 56/121 ГА ООН "Борьба с преступным использованием информационных технологий", а также региональные инициативы, включая, среди прочего, Конвенцию о борьбе с киберпреступностью Совета Европы;

c) что существенные потери, которые понесли системы на базе ИКТ в связи с возрастающей во всем мире проблемой киберпреступности, должны стать сигналом тревоги для всего международного сообщества, и особенно МСЭ;

d) необходимость решения с применением многостороннего подхода, включая международное сотрудничество, проблемы, связанной с кибербезопасностью, включая борьбу со спамом, которой не уделялось необходимое приоритетное внимание, к чему призывает Тунисская программа (пункт 41);

e) причины, предопределившие принятие Резолюции 37 (Стамбул, 2002 г.) Всемирной конференции по развитию электросвязи по преодолению "цифрового разрыва", принимая во внимание направления деятельности, указанные в пункте 108 Тунисской программы, в том числе "Укрепление доверия и безопасности при использовании ИКТ",

напоминая

a) стремление и решимость всех заинтересованных сторон построить ориентированное на интересы людей, открытое для всех и направленное на развитие информационное общество на основе целей и принципов Устава Организации Объединенных Наций, международного права и принципа многосторонних отношений, соблюдая в полном объеме и поддерживая Всеобщую декларацию прав человека, с тем чтобы люди во всем мире могли создавать информацию и знания, иметь к ним доступ, пользоваться и обмениваться ими, для того чтобы в полной мере раскрыть свой потенциал и

реализовать согласованные на международном уровне цели и задачи в области развития, включая Цели в области развития, сформулированные в Декларации тысячелетия;

b) положения пунктов 4, 5 и 55 Женевской декларации принципов и тот факт, что свобода слова и свободный поток информации, идей и знаний благоприятствуют развитию;

c) что Тунисская встреча на высшем уровне явилась уникальной возможностью для повышения уровня информированности о преимуществах, которые ИКТ могут дать человечеству, и о том, как они могут изменить деятельность, взаимоотношения и жизнь людей и, таким образом, укрепить уверенность в будущем,

признавая

a) положения о неприкосновенности частной жизни и свободе слова, которые содержатся в соответствующих частях Всеобщей декларации прав человека (пункт 42 Тунисской программы);

b) необходимость защиты этических аспектов информационного общества в соответствии с Женевскими декларацией принципов и планом действий (пункт 43 Тунисской программы), необходимость борьбы против терроризма (пункт 44 Тунисской программы) и важность непрерывного и стабильного функционирования интернета (пункт 45 Туниской программы), при обеспечении неприкосновенности частной жизни и защиты личной информации и личных сведений (пункт 46 Тунисской программы);

c) необходимость эффективного противодействия вызовам и угрозам, возникающим в результате использования ИКТ в целях, которые несовместимы с задачами по поддержанию международной стабильности и безопасности и могут оказать негативное воздействие на целостность инфраструктуры в рамках отдельных государств в ущерб их безопасности, и что необходимо действовать с целью предотвращения злоупотребления информационными ресурсами и технологиями в преступных и террористических целях и соблюдать права человека;

d) роль ИКТ в деле защиты детей и содействия их развитию, и что следует активизировать деятельность по защите детей от растления и защищать их права в контексте ИКТ, подчеркивая, что важнейшее значение имеет максимальное соблюдение интересов ребенка,

отмечая,

a) что Резолюция 50 (Флорианополис, 2004 г.) Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ) по кибербезопасности посвящена исключительно исследованию технических аспектов уменьшения воздействия этого явления;

b) что спам представляет собой крупную и возрастающую проблему для пользователей, сетей и интернета в целом и что вопросы спама и кибербезопасности следует решать на соответствующем национальном и международном уровнях,

настоятельно призывает Государства – Члены Союза

предоставить необходимую поддержку в выполнении настоящей Резолюции,

решает поручить Директору Бюро развития электросвязи

1 организовать, в соответствии с Программой 3 и на основе вкладов членов, собрания Государств – Членов Союза и Членов Сектора для обсуждения путей повышения кибербезопасности, включая, среди прочего, заключение МоВ между заинтересованными Государствами – Членами Союза с целью повышения кибербезопасности и борьбы со спамом;

2 представить отчет о результатах этих собраний Полномочной конференции (Анталия, 2006 г.).