ОБСЕ

Организация по безопасности и сотрудничеству в Европе
Постоянный совет

PC.DEC/991
31 March 2011

RUSSIAN
Original: ENGLISH

856-е пленарное заседание
PC Journal No. 856, пункт 3 повестки дня

РЕШЕНИЕ № 991
КОНФЕРЕНЦИЯ ОБСЕ ПО ВСЕОБЪЕМЛЮЩЕМУ ПОДХОДУ К КИБЕРБЕЗОПАСНОСТИ: ОПРЕДЕЛЕНИЕ БУДУЩЕЙ РОЛИ ОБСЕ

Постоянный совет,

ссылаясь на Решение № 3/04 Совета министров о борьбе с использованием Интернета в террористических целях, в котором содержался призыв к государствам-участникам обмениваться информацией об использовании Интернета в террористических целях и определять возможные стратегии борьбы с этой угрозой,

ссылаясь на Решение № 7/06 Совета министров о противодействии использованию Интернета в террористических целях, в котором выражалась обеспокоенность государств-участников продолжающимися актами хакеров и которое призывало их к принятию надлежащих мер по защите критических и жизненно важных объектов информационной структуры и информационных сетей от угрозы кибернападения,

ссылаясь на Решение № 9/07 Совета министров, которым был еще более расширен мандат ОБСЕ с включением в него также борьбы с сексуальной эксплуатацией детей в Интернете,

ссылаясь на Решение № 9/09 Совета министров о борьбе с преступлениями на почве ненависти, в котором содержался призыв, в частности к государствам-участникам, изыскивать возможности для решения проблемы все более широкого использования Интернета для пропагандирования мнений, представляющих собой подстрекательство к насилию, в том числе в форме преступлений на почве ненависти, обеспечивая при этом, чтобы любые надлежащие меры принимались в соответствии с обязательствами ОБСЕ, в частности, в отношении свободы выражения мнений,

ссылаясь на Решение № 10/08 Форума по сотрудничеству в области безопасности относительно рабочего совещания ОБСЕ по всеобъемлющему подходу ОБСЕ к повышению кибербезопасности, и принимая к сведению итоги этого мероприятия, включая рекомендации и предложения, распространенные в документе FSC.DEL/92/09,

ссылаясь на дискуссии по вопросу кибербезопасности в рамках корфуского процесса,

ссылаясь на Решение № 2/09 Совета министров, в котором подчеркивалась решимость государств-участников вести поиск решения проблемы кибербезопасности как транснациональной угрозы и вызова безопасности и стабильности, и принимая к сведению доклад Генерального секретаря ОБСЕ о выполнении Решения MC.DEC/2/09 о дальнейших усилиях ОБСЕ по противодействию транснациональным угрозам и вызовам безопасности и стабильности (SEC.GAL/107/10), в котором были наглядно показаны возможные варианты более активной роли Организации во всеобъемлющем повышении кибербезопасности,

ссылаясь на сообщения и дискуссии, имевшие место на 45-м совместном заседании ФСБ–ПС 2 июня 2010 года, на котором, среди прочего, была рассмотрена потенциальная роль ОБСЕ как платформы для обмена мнениями между странами о нормах, регулирующих поведение государств в киберпространстве,

принимая во внимание усилия, инициативы и инструменты других региональных и международных субъектов, которые ведут работу в областях, касающихся кибербезопасности, – и в первую очередь на уровне Организации Объединенных Наций – и желая при необходимости дополнить, расширить и совершенствовать прилагаемые в настоящее время усилия, избегая при этом ненужного дублирования,

учитывая постоянный интерес Организации Объединенных Наций, в частности, прослеживаемый в докладе по достижениям в сфере информации и телекоммуникаций в контексте международной безопасности (A/65/201), который был подготовлен в 2010 году группой правительственных экспертов, учрежденной в соответствии с пунктом 4 резолюции 60/45 Генеральной ассамблеи,

признавая, что угрозы, исходящие от киберпространства, и меры, направленные на повышение кибербезопасности, входят в число неотложных вопросов безопасности, волнующих государства-участники,

с озабоченностью отмечая, что угрозы, исходящие от киберпространства, постоянно эволюционируют и возрастают быстрыми темпами,

признавая, что для соответствия и впредь потребностям и интересам государств-участников, деятельность ОБСЕ по нахождению ответа угрозам, исходящим от киберпространства, должна эволюционировать в соответствии с характером угрозы, и отмечая соответствующую деятельность на уровне всего пространства ОБСЕ, а также на региональном и национальном уровнях по повышению осведомленности и созданию потенциала, которая реализуется усилиями ряда структур ОБСЕ,

признавая, что взаимосвязи между различными аспектами современных угроз, исходящих от киберпространства, требуют всеобъемлющего подхода к кибербезопасности,

вновь подтверждая, что уважение прав человека и основных свобод, демократии и верховенства права занимает центральное место в принятой ОБСЕ всеобъемлющей концепции безопасности и что при принятии усилий по повышению кибербезопасности следует в полной мере соблюдать основные свободы, такие, как свободу мнений и свободу выражения, включая свободу искать, получать и распространять информацию, которые жизненно важны для демократии и фактически укрепляются Интернетом и верховенством права,

вновь подтверждая, что ОБСЕ может действовать как платформа для диалога по вопросам безопасности, основанной на сотрудничестве, между государствами-участниками, а также региональными и международными субъектами, занятыми в этой тематической области, включая обмен мнениями о нормах и поведении государств,

поручает Генеральному секретарю организовать конференцию ОБСЕ по всеобъемлющему подходу к кибербезопасности: определения будущей роли ОБСЕ и провести ее 9–10 мая 2011 года в Вене с участием соответствующих международных субъектов и представителей частного сектора, а также в соответствии с общим замыслом, прилагаемым к настоящему Решению;

предлагает государствам-участникам рассмотреть возможность предоставления внебюджетных взносов на проведение вышеуказанного мероприятия.

PC.DEC/991
31 March 2011
Annex

КОНФЕРЕНЦИЯ ОБСЕ ПО ВСЕОБЪЕМЛЮЩЕМУ ПОДХОДУ К КИБЕРБЕЗОПАСНОСТИ: ОПРЕДЕЛЕНИЕ БУДУЩЕЙ РОЛИ ОБСЕ

Вена, 9–10 мая 2011 года

Конференция ОБСЕ по всеобъемлющему подходу к кибербезопасности: определение будущей роли ОБСЕ будет посвящена поиску возможного пути вперед в этой тематической области.

Мероприятие будет состоять из двух частей:

Часть I Конференции будет посвящена наглядной демонстрации примеров и повышению осведомленности относительно различных угроз кибербезопасности, которые связаны с: a) военно-политической областью, включая критически важные объекты информационной инфраструктуры, характер и возможные сферы охвата норм поведения в киберпространстве; и b) киберпреступностью и использованием Интернета в террористических целях, с определением характера потенциальных контрмер, извлеченных уроков и наилучших примеров национальной практики, в отношении также расследования и судебного преследования, формирования государственно-частных партнерств и эффективного вовлечения гражданского общества.

Часть II Конференции будет посвящена определению потенциальных ответных мер на киберугрозы и рассмотрению целесообразности разработки норм поведения государств, которые могли бы содействовать повышению кибербезопасности, а также мер, которые могут снизить неправильное восприятие и риски, включая меры укрепления доверия, учет соответствующих прав человека, мер по повышению стабильности и сокращению рисков, обмен информацией, например, относительно соответствующей правовой базы и, в частности, будут высвечены достижения и инициативы на глобальном и региональном уровнях, в первую очередь, роль других региональных организаций в этой сфере.

Заседание, посвященное закрытию, будет использовано для прогнозирования потенциальной будущей роли ОБСЕ и более конкретно тому, могут ли и каким образом инициативы на глобальном и региональном уровнях еще более активизированы благодаря усилиям ОБСЕ, в том числе путем принятия мер по созданию потенциала, и определения того, какие пробелы в потенциале могут быть восполнены посредством инициатив ОБСЕ, в том числе в свете рекомендаций, которые были даны соответствующей группой правительственных экспертов Организации Объединенных Наций[1].

1 Доклад группы правительственных экспертов по достижениям в сфере информации и телекоммуникаций в контексте международной безопасности (A/65/291).

В целом проведение Конференции направлено на решение следующих задач:

– наглядно продемонстрировать, как различные формы и методы противозаконного использования киберпространства, различные злоумышленники и преследуемые ими цели и соответствующие контрмеры и ответные шаги, в частности, со стороны международных и региональных организаций, влияют на безопасность в регионе ОБСЕ;

– определить имеющийся у ОБСЕ потенциал для внесения качественного значимого вклада в прилагаемые ныне усилия путем применения всеобъемлющего подхода к кибербезопасности, в том числе через обмен мнениями на национальном уровне и возможную разработку норм, регулирующих поведение государств в киберпространстве;

– создать базу для определения будущей роли Организации в этой тематической области и того, как в целом можно в потенциале еще больше повысить ее авторитет, исходя из дискуссий, рекомендаций и итогов ранее проведенных совещаний ОБСЕ;

– рассмотреть те шаги, которые, возможно, необходимо принять как на организационном уровне, так и в политических рамках, и того, могут ли инициативы на глобальном и региональном уровнях быть еще более активизированы путем использования сильных сторон ОБСЕ, которые связаны с мерами укрепления доверия, обменом извлеченными уроками, созданием потенциала и популяризацией наилучшей практики, – возможно, через подготовку стратегического документа ОБСЕ.

Секретариат ОБСЕ подготовит доклад о последующих шагах, в котором будут кратко изложены конкретные предложения и рекомендации, высказанные на этом мероприятии относительно будущей роли ОБСЕ в области всеобъемлющего повышения кибербезопасности и относительно возможных мероприятий в рамках последующих шагов силами соответствующих структур ОБСЕ в дополнение к международным усилиям в этой области.