Информационная безопасность для развития России

16:14 12/12/2013 Григорий Поволоцкий , шеф-редактор журнала «Международная жизнь»

В Аналитическом центре при Правительстве РФ 11 декабря с.г. состоялся круглый стол «Информационная безопасность как условие устойчивого и стабильного развития России», в котором приняли участие известные представители экспертного сообщества, ученые, представители Министерства обороны, МИД России других ведомств. Это было совместное мероприятие Аналитического центра при Правительстве РФ и Института Международных исследований ИМИ МГИМО (У) МИД России при содействии редакции журнала «Международная жизнь». На открытии мероприятия присутствовала заместитель директора Аналитического центра при Правительстве России Галина Чинарихина.

Со вступительным словом к участникам круглого стола обратился руководитель Дирекции по информационным технологиям Аналитического центра при Правительстве Российской Федерации Алексей Хромов. А.Хромов подчеркнул, что проблемы информационной безопасности в свете стремительного развития информационного общества становятся все более актуальными. Пожелав всем участникам плодотворной дискуссии, руководитель Дирекции предложил, чтобы итогом обсуждения, возможно, стало одобрение собравшимися предложения Аналитического центра при Правительстве РФ и Института международных исследований о проведении международную конференцию по информационной безопасности в городе Москве

весной следующего 2014 года.

С кратким вступительным словом обратился к собравшимся также Чрезвычайный и Полномочный Посланник, директор Института международных исследований МГИМО (У) МИД России А.Орлов. Роль информационной сферы в жизнедеятельности современного общества постоянно возрастает, отметил он. Это – объективный процесс, который невозможно остановить. Доступ современного человека к информации является непреложным условием гармоничного развития личности, отражением его конституционных прав. В последние годы в нашей стране осуществлен комплекс мер, направленных на обеспечение информационной безопасности. Именно в этих целях, как подчеркнул А.Орлов, формируется необходимое правовое пространство, принят ряд законов и нормативных актов в этой области. Президентом России утверждены Доктрина информационной безопасности РФ и Стратегия развития информационного общества в РФ.

Информационная безопасность становится полем широкого международного сотрудничества. Одна только Генеральная Ассамблея ООН приняла более десятка резолюций по этому вопросу.

В то же время, заметил ученый, открытостью информационной среды в наши дни активно пользуются те, кто стремится к дезорганизации общества, разжиганию социальной, расовой, национальной и религиозной ненависти и вражды, кто задался целью вторгаться в частную жизнь и переписку граждан с неблаговидными целями. Неточная или сознательно искаженная информация, являющаяся, как известно, формой косвенного управления, манипулирования, как человеком, так и обществом в целом, способна провоцировать или усиливать социальную напряженность, что может вести к непредсказуемым и даже трагичным последствиям. Откровения Эдварда Сноудена о плотном «электронном колпаке» установленном американскими спецслужбами над всем мировым сообществом (от простых граждан до лидеров государств, в том числе союзных Соединенным Штатам) высветили иную сторону информационной безопасности. Это сторона интернета связанна с границами допустимого вмешательства со стороны государства и его специальных органов в личную жизнь граждан, даже под внешне благовидным предлогом.

Россия весьма заинтересована в участии в решении задач по обеспечению безопасности использования информационных и коммуникационных технологий (ИКТ), стремится к налаживанию масштабного сотрудничества в деле укрепления мер доверия в сфере применения ИКТ и повышения эффективности переговорного процесса в области

формирования целостной системы международной информационной безопасности. Системное, углубленное изучение всех аспектов формирования новой информационной культуры человека и общества является в наше время одной из наиболее актуальных задач обеспечения национальной безопасности России, заключил руководитель Института международных исследований.

Завершив свое краткое выступление А.Орлов, как модератор круглого стола, предоставил слово заместителю директора Института проблем информационной безопасности МГУ им. М.В.Ломоносова Анатолию Стрельцову для доклада на тему «Правовое обеспечение информационной безопасности».

Заместитель директора Института проблем информационной безопасности отметил, что правовое обеспечение информационных технологий – один из важнейших вопросов повестки дня. Количество нормативно-правовых актов более чем велико, но качество их вызывает серьезные нарекания. Это и понятно - все депутаты Федерального собрания не могут быть специалистами в области права, становление норм которого пока еще даже не завершилось.

Директор ИМИ МГИМО МИД России А.Орлов, руководитель Дирекции по информационным технологиям Аналитического центра при Правительстве РФ

А.Хромов и заместитель директора Института проблем информационной безопасности МГУ им.М.В.Ломоносова А.Стрельцов.

Важно противодействие компьютерной преступности, отметил А.Стрельцов. Есть соответствующие подразделения и в ФСБ и в МВД, но нет пока снижения преступности. Такая же тенденция видна хорошо и в зарубежных странах, при том, что там тратят на борьбу с компьютерной преступностью на порядок или два больше средств, чем Россия. Необходимо, сделал предложение ученый, внести в Уголовный кодекс России изменения направленные на усиление ответственности, если преступление совершается при помощи информационно-компьютерных технологий.

Цель обеспечения государственной политики в сфере ИКТ –поддержка населением этих мероприятий. Мое предложение – при оценке деятельности власти главный показатель – поддержка в обществе.

А стрельцов с сожалением констатировал, что сегодня при Президенте России нет ни совета, ни комиссии по информационному обществу. Подобный институт, по мнению эксперта, помог бы привлечь общественное мнение к решению данной проблемы.

Затронув тему обеспечения безопасности объектов информационной инфраструктуры, А.Стрельцов отметил, что в настоящее время обсуждается Проект закона. Он обратил внимание на то, что обеспечить все это усилиями одних органов исполнительной власти – невозможно. Необходимы две составляющие- государство и негосударственные структуры. Как показывает практика, пояснил А.Стрельцов, эта проблема, к сожалению, пока не решена и в ведущих промышленных странах мира, например, в Германии.

В заключительной части своего выступления Заместитель директора Института проблем информационной безопасности МГУ им. М.В.Ломоносова коснулся вопросов международной проблематики. По его мнению необходима международного права к разрешению межгосударственных противоречий в сфере информационных технологий.

Следующая выступающая, Мадина Касенова, Заведующая кафедрой международного частного права Дипломатической академии МИД России , затронула вопросам формирования модели трансграничного управления интернетом и сотрудничества

государств в сфере безопасного использования интернета.

М.Касенова акцентировала свое выступление на международно-правовом контексте. Она отметила что принятые осенью Основы государственной политики ставят внешнюю канву и дают исходные позиции для развития российской позиции. По мнению М.Касеновой можно говорить о том, что интернет сегодня никому не принадлежит и во многом превращается в полигон технологической «гонки вооружений» в сфере ИКТ. Из этого следует такие парадоксы, что, например, «государство Тувалу более защищено от хакерских атак и вторжений, чем США» [*поскольку, возможно, что в Тувалу интернета нет вообще…- Прим.авт.*]. Существует международное право войны и международное право мира. Мир может и должен начать обсуждать ограничения правил ведения «кибервойн» вместо обсуждения вопросов мирного использования интернета, считает Заведующая кафедрой международного частного права Дипломатической академии МИД России. По мнению М.Касеновой необходимо обсуждать вопросы безопасности ИКТ на многих международных площадках и, например, активнее делать это в рамках ОБСЕ.

С докладом «Международная безопасность в области использования ИКТ: глобальные тенденции и национальные интересы России» выступил Олег Демидов, Директор программы ПИР-Центра «Международная информационная безопасность и глобальное управление интернетом»

Выступивший О.Демидов постарался ответить на вопрос: готова ли Россия к решениям международного технического сообщества об управлении интернетом. Он отметил что ведутся дискуссии на разных международных площадках, обсуждаются политические механизмы, предлагаются новые механизмы защиты частной жизни для пользователей мировой сети. К сожалению Россия не участвует в таких дискуссиях. Есть ли диалог России с этими экспертными площадками? Есть ли реакция на те пороки, но которые указал Эдвард Сноуден?

Сегодня, как известно, одна организация раздает IP-адреса и доменные имена, а именно «Internet Corporation for Assigned Names and Numbers» (ICANN) [*международная некоммерческая организация, созданная*
18 сентября

1998 года
 при участии правительства
США

для регулирования вопросов, связанных с доменными именами, IP-адресами и прочими аспектами функционирования Интернета – Прим.авт.
]. Был ли ей дан международный мандат? – задается вопросом ученый. ICANN, по его мнению, сегодня больше похожа на акционерное общество. Сегодня считает ученый, организация поворачивается к миру и уходит из-под опеки США.

Другой важный по его мнению вопрос – вопрос ближайшей перспективы развития международного гуманитарного права. Уже был печальный опыт создания экспертами НАТО т.н. «Таллиннского руководства». Это была системная попытка ответа на применение гуманитарного права в конфликтах в киберпространстве.

У нас отсутствует определение кибероружия, отметил О.Демидов. Это глобальный вопрос который входит и в проблематику России (индоктринирование в систему вооруженных сил России). Существуют общие определения: информационные операции, защита компьютерных сетей. Как все это надо называть с точки зрения военных? Ведь оборона собственного киберпространства – это часто активные операции в чужих сетях. А как это сопоставлять с оборонной доктриной России? Как определить в терминах, кого должно защищать российское киберкомандование вместе с ФСБ России? Таким образом, по мнению выступающего, один из наиболее важных вопросов повестки дня – вопрос терминологии.

Следующий выступающий, Виталий Каберник, Начальник отдела перспективных научно-образовательных разработок Управления инновационного развития МГИМО (У) МИД России в своем докладе коснулся вопросов наступательного потенциала в киберпространстве.

В.Каберник определяет киберпространство как пространство кибернетических систем, которое может быть и не сетевым. При этом в ряде случает подчеркнул выступающий, отдельные не сетевые системы могут подвергаться заранее преднамеренному внедрению закладок, и т.д. Что такое кибероружие и кибервойна? По мнению докладчика понятие «кибервойна» не существует, эту терминологию нам пытаются внедрить с Запада. Таких войн быть не может, война сегодня не может быть ограничена каким-то одним видом техники (скажем «бронетранспортерная война», «пистолетная

война»). Расширение средств ведения войны - это, по мнению докладчика, аксиома известная всем со времен Клаузевица и даже ранее. Запад предлагает нам взаимопротиворечащее определение с тем, чтобы внести путаницу. Впрочем, по мнению ученого, вопрос о преднамеренности открыт.

Что представляет из себя кибероружие – вирусы, различные хакерские атаки, внедрения – это один из пластов. Если сегодня для нападения используются киберсети, это происходит очень быстро, буквально мгновенно и на такое воздействие нет сдерживающего потенциала. Это приравнивает кибероружие по ряду параметров к стратегическим наступательным вооружениям (СНВ).

Если посмотреть на устройство современной армии, то, как считает В.Каберник, сегодня в войсках в плане кибероружия явно провалено тактическое звено – не хватает соответствующих специалистов, но на стратегическом уровне разработки воздействия есть.

Можно ли ставить вопрос о демилитаризации интернета? Возможно, но сейчас это нереализуемая задача. Есть перспектива регулирования киберпространства с точки зрения вылавливания на черных рынках продаваемого кибероружия. При этом доктрина обороны должна строится на своей элементной базе, так как несетевые атаки никто не отменял.

С докладом «Принцип участия всех заинтересованных сторон в определении национальных интересов России в сфере ИКТ: дань моде или практическая потребность?» выступил Михаил Якушев, международный эксперт, преподаватель Дипломатической академии МИД России, член Совета Координационного центра национального домена сети Интернет

Якушев отметил, что в 2003 году вопрос о контроле над интернетом уже обсуждался на проводившемся в Женеве саммите по проблемам информационного общества. Однако к единому мнению его участники не пришли, и при ООН была организована рабочая группа по управлению интернетом (РГУИ), которой поручили разработать варианты международного управления интернетом. В июле 2005г. работа комиссии успешно завершилась. Ее итогом стал документ, в котором предложены четыре модели международного управления интернетом.

Но что такое интернет? Определение интернета включает принцип участия всех заинтересованных сторон – государственных организаций, частного сектора, гражданского общества и еще добавляют экспертного сообщества. Создание и освоение интернета человеком по сложности задачи можно приравнять к задаче освоения космоса. Так огромен и бесконечен информационный мир. Как все это должно работать? К сожалению, пока нет даже общего понимания понятийного аппарата. И, конечно, важна недопустимость слежки в интернете. Один из важных вопросов – вопрос идентификации пользователей интернета. Недопустимо говорить об абсолютной анонимности, но и нельзя пускать в интернет «по паспорту».

На каком уровне регулируется интернет (подключение, отключение или уничтожение)? Пока на уровне приложений, где осуществляется национальное регулирование. На более высоком уровне – сетевые адреса, доменные имена, и еще более высоком – на сетевом уровне, регулирования нет.

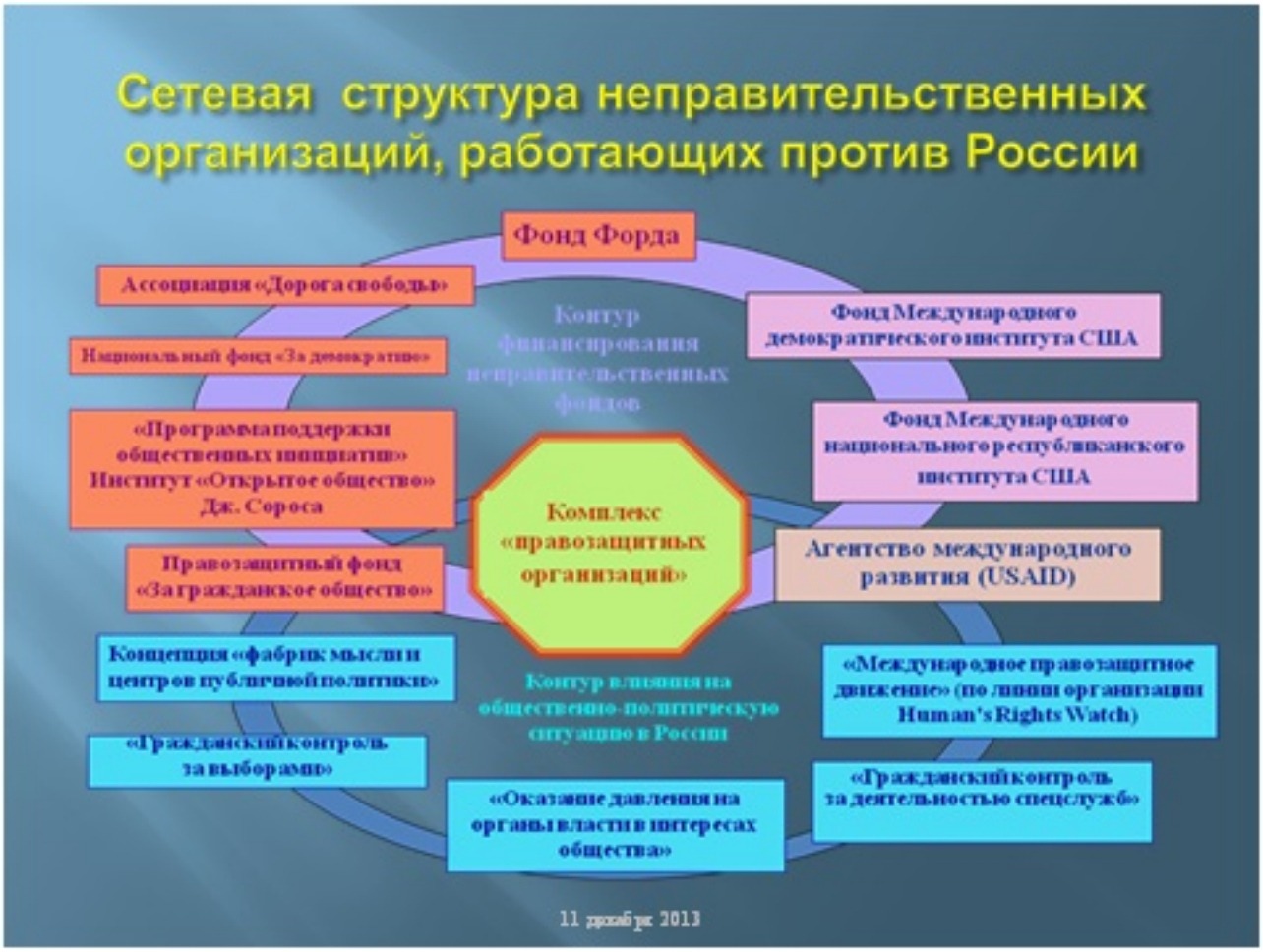
ICANN регулирует домены, сетевые адреса регулируют 5 организаций в мире. Организация регулирующая сетевые адреса по России находится в Амстердаме и действует по голландскому праву…

Можно и нужно искать нарушителей интернета. Есть разные методики. Но важнее всего сегодня, по мнению М.Якушева, фильтрация на уровне семьи.

Россия, по мнению М.Якушева, недостаточно активно использует свои международные возможности – необходимо активно участвовать в работе всех международных площадок, а не уходить от них.

Следующим выступающим стал Чрезвычайный и Полномочный Посланник РФ, Президент-председатель Научного совета Национального института исследований глобальной безопасности Анатолий Смирнов, представивший свой доклад «Стратагема международной информационной безопасности» в виде яркой и содержательной презентации.

Как напомнил участникам дискуссии А.Смирнов, «Смена исторических эпох определяется сменой коммуникационных технологий» (Герберт Маршалл Маклюэн). По его мнению начало XXI в. может войти в скрижали человечества как один из самых драматичных периодов. Планета вошла в зону геополитической турбулентности: сполохи войны цивилизаций, международного терроризма, угроза рецессии, рецидивы холодной войны и пиратства, всплеск локальных и региональных конфликтов, техногенные, природогенные, социогенные катастрофы, эпидемии и пандемии, голод. Наиболее емко эта ситуация оценена в Стратегии национальной безопасности России (от 12.05.2009г.): «Возросла уязвимость всех членов международного сообщества перед лицом новых вызовов и угроз». Появились и инфогенные угрозы.



Слайд из доклада-презентации Президент-председатель Научного совета Национального института исследований глобальной безопасности А. Смирнова

Более полувека весь мир, отметил А.Смирнов, охвачен беспрецедентной информационной революцией. Её феномен принципиально изменил геополитический код цивилизации: с одной стороны – локомотив пятого технологического уклада, с другой – новые вызовы и угрозы международной безопасности. Ведущие государства разработали и реализовали концептуальные и доктринальные стратагемы использования потенциала ИКТ в геополитической конкуренции.

Известный эксперт напомнил о том, что Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». (Утверждены Президентом РФ 24 июля 2013 г. Пр-1753) к числу основных приоритетов относят участие России в формировании механизмов международного сотрудничества в области противодействия угрозам использования ИКТ в террористических и экстремистских целях, в т.ч. для вмешательства во внутренние дела суверенных государств. В целом Основы закрепляют стремление Российской Федерации к масштабному сотрудничеству в деле укрепления мер доверия в сфере применения ИКТ и повышения эффективности переговорного процесса в области формирования системы международной информационной безопасности (МИБ).

К каким выводам и предложениям приходит руководитель Научного совета Национального института исследований глобальной безопасности? Прежде всего, считает А.Смирнов, необходимо использовать мощный потенциал экспертного сообщества России для продвижения МИБ. А.Смирнов также поддержал предложение о проведении конференции международной конференции по информационной безопасности в Москве, равно как и предложение, высказанное А.Стрельцовым, о привлечении общественности, т.е. краудсорсинга. Он также предложил создать закрытую социальную сеть для экспертов по вопросам информационной безопасности.

Большой интерес вызвал доклад о система кибероборонь КНР, который сделал старший научный сотрудник Центра анализа стратегий и технологий Василий Кашин

Как отметил В.Кашин, осознание роли информационных технологий и кибероружия в КНР началось в 90-е годы прошлого 20-го века, когда на эту тему появился ряд публикаций в военных журналах, оценивающих такие процессы в США. Новый рывок НОАК совершает в 2000 году: 4-е управление (радиоэлектронной борьбы - РЭБ) Генштаба КНР начинает разработку интегрированных электронно-сетевых операций в качестве приоритетных с тем, чтобы нивелировать американское военное превосходство.

Первые данные об успехах НОАК появились в 2004 году, когда было сообщено об учениях киберподразделений 38 и 65 армий НОАК, которые демонстрировали свои возможности стремясь в ходе учений одолеть друг друга.

Растет численность 4-е управления Генштаба КНР, которое взаимодействует с 3-м управлением Генштаба КНР. Всего на направлении киберпротивоборства служат более 100 тыс. военнослужащих, что сопоставимо с численностью структур АНБ США.

На сегодня можно говорить о существовании 12 бюро техразведок ориентированных по географическому принципу. Видимо их часть и ведет киберпротивоборство с США. 3 техбюро ориентированы на Север (возможно, в том числе, на Россию и Монголию) - №№ 5,10,11. В КНР открыты как профильные высшие учебные заведения, так и лингвистические институты, готовящие пополнение для армейских специалистов. КНР создало объекты РЭБ-кибербезопасности на Кубе, в Пакистане и Иране.

Используя растущий потенциал китайского IT сектора экономики НОАК призывает на военные сборы специалистов, сохраняя тем самым значительный кадровый и материальный потенциал.

С докладом о Центр кибербезопасности НАТО в Таллинне выступил Генеральный директор «ИнфоРос» Денис Тюрин. В конце ноября в Эстонии прошли крупнейшие за время существования НАТО учения по отработке вопросов киберзащиты инфраструктуры Альянса «Cybercoalition-2013». В учениях приняло участие, подчеркнул выступавший, почти 500 человек: свыше 100 сотрудников таллиннского Объединенного центра передового опыта в области киберзащиты НАТО и еще более 300 офицеров из 32 стран-членов и партнеров Альянса - удаленно.

По мнению Д.Тюрина учения «Cybercoalition-2013» стали логическим продолжением военных маневров НАТО «Steadfast Jazz – 2013», которые проходили в начале ноября на территории Прибалтики и Польши. Сценарий этих маневров предусмат-ривал, помимо отражения агрессии против Эстонии со стороны вымышлен-ного государства "Ботния", в том числе и отработку защиты стран НАТО от масштабного кибердара предполагаемого противника. По удивительному совпадению, в самом начале учений государственные информационные ре-сурсы Украины, России, Польши и стран Прибалтики подверглись

вполне реальным, а не учебным хакерским атакам. На несколько часов прекратил работу даже сайт таллиннского Киберцентра НАТО. Кто стоял за этими атаками, так и осталось неясным.

С Украиной, по мнению Генерального директора «ИнфоРос», ситуация сложилась по-другому. На выведенных из строя сайтах украинских государственных структур (Генпрокуратура, мед- служба СБУ и др.) от имени таллиннского киберцентра НАТО было разме-щено предупреждение о несоответствии этих веб-страниц натовским стан-дартам кибербезопасности. Брюссель, конечно же, опроверг свою причастность к этим инциден-там. В самый разгар учений Таллиннский Центр киберзащиты НАТО офици-ально заявил о том, что некие силы просто прикрылись его добрым именем и постарались скомпрометировать деятельность Альянса. Виновник или ви-новники всего происшедшего так и не был названы.

Как считает Д.Тюрин, то, что не могут сделать официальные структуры, доступно экс-пертному сообществу. Особенно такому яркому его представителю как Меж-дународный центр оборонных исследований, расположенному все в том же Таллинне и возглавляемому небезызвестным специалистом по информацион-ным провокациям, отставным американским дипломатом Мэттью Брайзой.

Выступавший напомнил, что сам выбор Таллинна в качестве места расположения Центра кибербезопасности НАТО диктовался настоятельными просьбами Эстонии обезопасить ее от хакерских атак, сопровождавших массовые про-тесты против переноса "бронзового солдата" в 2007 г. Эстонские власти и то-гда увидели здесь "русский след" и потребовали у альянса усиленную кибер-нетическую защиту.

Россия, по мнению Д.Тюрина, пока объективно отстает от США и других стран НАТО в развитии собственной программы кибербезопасности. Заявленное создание кибервойск пока не произошло, об учениях по информационной безопасности вообще ничего не слышно. Не случайно, наверное, что именно Россия выступила в ООН с инициативой ограничения гонки вооружений в информационной сфере и предложила другим странам присоединиться.

Дискуссия, прошедшая в Аналитическом центре при Правительстве РФ была откровенной, интересной и весомой. Обсуждение вопросов показало с одной стороны необходимость регулярного проведения подобных встреч экспертов для обмена

мнениями, координации позиций. В этот раз, пожалуй, в выступлениях экспертов наиболее остро прозвучала проблема необходимости создания единой системы терминологии и ее кодификации. Состоявшаяся дискуссия стала определенным вкладом экспертного сообщества в разработку вопросов национальной безопасности применительно к ИКТ, обзором российских позиций по вопросу международной информационной безопасности. Вызывает удовлетворение тот факт, что участниками круглого стола одобрили инициативу Аналитического центра при Правительстве РФ и Института международных исследований ИМИ МГИМО (У) МИД России о проведении весной 2014 года международной конференции по информационной безопасности. При этом была отмечена важная роль которую может сыграть журнал «Международная жизнь» в качестве информационного спонсора такого события.

Источник: http://interaffairs.ru/read.php?item=10311