Наша Газета
nashagazeta.ch
Опубликовано на Швейцария: новости на русском языке (https://nashagazeta.ch)

Кибербезопасность и управление интернетом – взгляд из Женевы глазами международных экспертов | Cybersecurity and Global Internet Governance Discussed by International Experts in Geneva

Автор: Олег Демидов, Женева-Москва , 04.05.2012.

Тон дискуссии в Женеве задал российский эксперт Михаил Якушев

На прошлой неделе Женева стала площадкой для обсуждения вопросов безопасности и управления современными информационными технологиями. Организовал дискуссию Центр политических исследований России (ПИР-Центр).

|

The Russian Centre for Policy Studies (PIR Centre) held a discussion of the problems concerning cybersecurity and Internet governance. Key findings of the debate.
Cybersecurity and Global Internet Governance Discussed by International Experts in Geneva

Centre russe d’etudes politiques, европейская ветвь одного из ведущих в России неправительственных научно-аналитических институтов – Центра политических исследований России (ПИР-Центр), - в ходе международного семинара представил независимый взгляд российских экспертов на ключевые проблемы глобального управления интернетом и международной информационной безопасности.

Впрочем, в зале находились не только российские эксперты – ПИР-Центру удалось собрать широкую международную аудиторию для обмена мнениями с теми, кто непосредственно причастен как к управлению Сетью, так и к выработке национального и международного курсов различных стран в сфере кибербезопасности. В дискуссии в числе прочих приняли участие заместитель Постоянного представителя РФ в Женеве Виктор Васильев и его американский коллега Уолтер Рейд, руководитель Отдела корпоративной стратегии Международного союза электросвязи Александр Нтоко, вице-президент Общества Интернета (ISOC) Маркус Куммер. С развернутым комментарием выступил один из крупнейших европейских исследователей и теоретиков информационных технологий профессор Цюрихского университета Рольф Вебер.

Открывая дискуссию, Председатель Совета ПИР-Центра, вице-президент Mail.Ru Group и ведущий российский специалист по киберправу Михаил Якушев отметил чрезвычайную широту и сложность обсуждаемой повестки. Принципы, на которые опирается глобальное управление интернетом, отражают уникальную трансграничную и децентрализованную природу этой технологии, которая зачастую идет вразрез с традиционным пониманием суверенитета национальных государств и требует новых моделей международного сотрудничества, особенно с учетом молниеносных изменений и новаций, сопровождающих развитие интернета и киберпространства.

Во главе угла для многих экспертов и правительственных ведомств сегодня стоят вопросы трансформации глобальной архитектуры управления интернетом, меняющей привычную нам Сеть. Взрывообразный рост физических устройств, через которые осуществляется коммуникация наряду с увеличением количества и спектра каналов коммуникации на физическом уровне дал нам мобильную революцию в интернете, оттеснив ПК на второй план. Не менее радикальные преобразования грядут на уровне IP-адресов в связи с уже стартовавшим всеобщим переходом на новую версию IP протокола – от IPv4 к IPv6: результатом станет рост количества сетевых адресов с нынешнего предела в 4,23 млрд. (который был исчерпан 1 февраля 2011 г.) до практически неисчерпаемого уровня. Таким образом, становится практически осуществимой идея интернета вещей, в котором каждое бытовое устройство вплоть до холодильника, пылесоса и одежды, не говоря уже о мультимедийных гаджетах, получит собственный выход в Сеть и сетевой адрес. Емкость такого интернета оценивается в триллионы объектов – а значит, и триллионы адресов, которыми с легкостью обеспечит пользователей протокол IPv6. Собственная революция происходит и на третьем уровне сетевой архитектуры – в пространстве DNS-имен. Расширение и либерализация правил регистрации доменов верхнего уровня (TLDs) развеет последнюю иллюзию национального суверенитета в

интернете – нынешние страновые домены верхнего уровня (.ch, .ru, .uk) попросту потеряются среди новых верхних доменных зон, закрепленных за корпорациями, общественными объединениями да и просто проектами отдельных пользователей – такими как .microsoft, .facebook, .google, .religion, .luckilyman и т.д.

Подобные новации ставят все новые вопросы перед правительствами и международным сообществом, создавая объекты и системы отношений, для которых попросту не существует должной системы регулирования. К примеру, на сегодняшний день практически никак не регулируется деятельность социальных сетей, крупнейшая из которых – детище Марка Цукеберга Facebook, - уже стала третьим по населению «государством» мира с 900 млн. пользователей. Потенциал трансграничных, глобальных социальных сетей в полной мере проявил себя как в событиях Арабской весны, так и во время прошлогодних беспорядков в Лондоне. Вопрос в том, кем и какие именно меры регулирования в отношении социальных сетей должны быть приняты, чтобы ограничить потенциал их использования в негативных целях, и при этом не ущемлять права пользователей?

Отсюда вытекает один из ключевых, по словам господина Якушева, вопросов - кто именно должен рассматриваться в качестве субъектов глобального управления интернетом? По мнению самого спикера и других участников дискуссии, единственным ответом является модель мультистейкхолдеризма – или управления усилиями многих заинтересованных участников. В традиционную мультистейкхолдерскую модель включаются три субъекта – правительства, частный сектор и гражданское общество. Однако, как отметил вице-президент ISOC Маркус Куммер, сегодня к этой композиции все чаще добавляется в качестве отдельного равноправного субъекта сообщество технических и теоретических экспертов в области интернета. Суть модели, однако, от этого не меняется – предполагается равное и одинаково приоритетное участие всех заинтересованных сторон в выработке подходов к тому или иному аспекту управления интернетом и безопасности киберпространства.

Одна из главных проблем для России на сегодня заключается в частичном игнорировании этой модели, что отражается как на повседневной практике управления интернетом в стране, так и в ключевых российских инициативах, ориентированных на международное сообщество. Последним примером такой инициативы стала презентованная в октябре 2011 г. концепция Конвенции об обеспечении международной информационной безопасности – проект глобального международного документа, охватывающего все ключевые вопросы противодействия угрозам из киберпространства в широком российском понимании. Хотя концепция сама по себе не содержит фундаментальных идейных изъянов и вводит важные понятия, наподобие информационных войн, действий, направленных на подрыв суверенитета в информационном пространстве, информационных конфликтов и т.д., на международной арене она была встречена с изрядным скепсисом и недоверием. Причина, как пояснил господин Якушев, заключается как раз в том, что проект документа разрабатывался правительственными структурами в полной изоляции от частного сектора, экспертного сообщества и неправительственных организаций. В результате текст концепции Конвенции грешит неточностями, некорректно подобранными определениями и просто неподходящими формулировками – при том, что в документе итак продвигается расширенное российское понимание информационной безопасности, не самое понятное для западных коллег Москвы, привыкших говорить о более узкой и традиционной проблематике

кибербезопасности. Последняя де-факто ограничена вопросами безопасности компьютерных систем, тогда как информационная безопасность в видении Москвы помимо компьютерной составляющей вбирает в себя диверсионные и психологические операции в информационном пространстве, контроль над медиапространством и ресурсами масс медиа, радиоэлектронную борьбу и идеологическое доминирование. Неудивительно, что такая расширительная трактовка вкупе с терминологическими огрехами позволила критикам Конвенции говорить о наличии в ней инерции конфронтационного мышления в духе Холодной войны.

Вместе с тем, как подчеркнул господин Якушев, концепция затрагивает – хотя и не решает полностью - принципиальный вопрос о том, какие уровни и сферы конфликтов в киберпространстве должны стать предметами международной повестки. Кибервойны, которые ведутся государствами против государств, являются лишь верхним уровнем «пирамиды» подобных конфликтов; в ее основании – «обычная» киберпреступность – действия граждан против граждан. Еще одним уровнем кибертерроризма является деструктивная активность граждан, направленная против государства и общества в целом. Однако есть и четвертый уровень, который до сих пор остается в тени как на международной арене, так и в национальной повестке информационной безопасности – действия государств и аффилированных с ними субъектов против отдельных граждан. Примерами могут служить атаки на ресурсы оппозиционных деятелей и представителей независимых СМИ в ряде авторитарных государств; в аналогичных действиях неоднократно, хотя и бездоказательно, обвинялись и российские власти. Вынесение этого «уровня» киберконфликтов в поле международной дискуссии необходимо, ведь только так можно выстраивать сотрудничество по противодействию полному спектру угроз, исходящих из киберпространства – и ПИР-Центр на сегодняшний день является единственной неправительственной организацией, работающей с этой проблемой.

Наконец, весьма важным и перспективным механизмом выстраивания общего международного режима управления интернетом и противодействия угрозам из киберпространства являются инструменты так называемого мягкого права (soft law). Хорошим примером таких механизмов, по словам господина Якушева, стали акты связанных с регулированием интернета, принятые 21 сентября 2011 г. Комитетом министров Совета Европы. Несмотря на то, что акты не имеют силы международного договора, а Совет Европы не является глобальной организацией, именно такие инструменты являются наиболее подходящей базой для последующих нормативных новаций в области транснационального киберправа.

Комментируя выступление Председателя Совета ПИР-Центра швейцарский профессор Рольф Вебер подчеркнул несколько моментов, связанных с историческими тенденциями развития интернета и определяющими его сегодняшнюю логику и закономерности развития. Во-первых, интернет проделал огромный путь от управления, сконцентрированного в едином частном центре, к многосубъектной модели – но этот путь не закончен. ICANN, ключевая структура в нынешней системе управления интернетом, нуждается в дальнейшем реформировании и более прозрачной и ответственной модели деятельности. Подтверждением этому служит недавний инцидент 19 марта 2012 года. В ходе введения в действие новых доменов верхнего уровня (TLDs) возникла серьезная угроза безопасности - произошла утечка данных авторов заявок на новые доменные имена и зоны. Реакция ICANN оказалась далека от идеальной – корпорация предпочла отделаться дежурными заявлениями о

«принятии всех необходимых мер», не предоставив ни инструкций по действиям для пострадавших субъектов, ни данных об ответственных за инцидент. Ситуация стала отличным примером того, в каких случаях должен расширяться объем ответственности управляющей структуры – ведь в конечном счете неизвестен остался даже объем ущерба, нанесенного в результате данного сбоя. Подобные случаи лишь подтверждают необходимость взглянуть на актуальные вопросы глобального управления интернетом с позиций деятельности ICANN в целом.

Как выяснилось в ходе дискуссии, вопросы кибербезопасности имеют самое прямое отношение и к ее участникам: как отметила главный редактор швейцарской «Нашей Газеты.ch» Надежда Сикорская, в феврале этого года сайт издания был выведен из строя мощными атаками и почти уничтожен. По словам Владимира Орлова, сайт ПИР-Центра в декабре 2011 года также подвергся DDoS-атакам, осуществлявшимся с территории одного из государств СНГ. Результаты расследования инцидентов, которые в обоих случаях до сих пор не привели к конкретным результатам и не стали поводом для возбуждения уголовных дел, стали лишним подтверждением того, что международному сотрудничеству в обеспечении кибербезопасности еще есть куда развиваться, а организованная ПИР-Центром дискуссия далеко не напрасна.

Как отметил заместитель Постоянного представителя РФ при Европейском отделении ООН в Женеве Виктор Васильев, опыт России в обеспечении информационной безопасности следует рассматривать положительно. Именно с российской подачи вопросы информационной безопасности на международном уровне получили развитие в повестке ООН уже в 1998 году, и с тех пор РФ активно и системно продвигала эти вопросы, активно участвуя в работе экспертных групп Генеральной Ассамблеи, ЮНИДИР и других структур Организации. Кроме того, Россия, в отличие от многих других государств, никогда не прибегала к использованию «красной кнопки» - т.е. полной блокировки интернета в крупных масштабах. Как отметил господин Васильев, использование «красной кнопки» сегодня представляет собой важный вопрос в контексте реагирования на кризисные ситуации. Где проходят границы легитимного и правомерного применения этого инструмента? Можно ли отключать интернет лишь тогда, когда его противоправное использование осуществляется вне контекста массовых политических и гражданских движений, борьбы за гражданские права, как, например, в ходе «Арабской весны» в 2011 году? Можно ли блокировать мобильную связь из тех же соображений, например, в России, где северокавказские боевики зачастую совершают теракты, приводя в действие взрывные устройства при помощи СМС и мобильных звонков? Ситуация далеко не однозначна и требует отдельного подхода в каждом случае, отметил господин Васильев.

Однако еще более важна, по мнению зампостпреда, задача поиска общих интересов и целей, выработки совместного видения проблем и вызовов в части информационной безопасности – как на широкой международной арене, включая площадки ООН, МСЭ и ВТО так в двустороннем формате с ключевыми партнерами РФ. Круг вопросов, которые интересны России, во многом касается кибермошенничества и финансовых преступлений, осуществляемых при помощи ИКТ – взлома и кражи данных кредитных карт, атак на системы онлайн-банкинга; в повестке дня также должны быть противодействие распространению в интернете детской порнографии.

Эту точку зрения поддержал зампостпреда США при ООН в Женеве Уолтер Рейд, отметив высокий приоритет поиска общей повестки в области информационной

безопасности между США и РФ. Задача двух держав сейчас состоит в максимальной активизации стратегического диалога по вопросам кибербезопасности за счет мер по укреплению доверия, и соответствующая почва здесь уже заложена, считает господин Рейд. Несмотря на действительно существующую проблему с отсутствием единой согласованной терминологии, Москве и Вашингтону уже много раз удавалось приходить к консенсусу по отдельным вопросам в этой сфере. Одним из последних прорывов стало совместное заявление замсекретаря российского Совбеза Н.В.Климашина и Координатора Белого Дома по кибербезопасности Г.Шмидта от 28 июня 2011 года, в котором содержался перечень планируемых двусторонних мер и механизмов укрепления доверия и обмена информацией о киберинцидентах и киберугрозах. Интересам США также в полной мере отвечает продвижение мультистейкхолдерского подхода к управлению интернетом в развивающихся странах – в том числе, в России. Устойчивый и конструктивный диалог двух стран невозможен без интенсивного и системного взаимодействия их гражданского общества и частного сектора, формирующих общее видение проблем и интересов в сфере кибербезопасности на неправительственном уровне.

Олег Демидов - младший научный сотрудник Центра политических исследований России (ПИР-Центр), Москва.

кибербезопасность
Женева
Статьи по теме
Швейцарцы также пострадали от хакеров Anonymous
Швейцария под прицелом хакеров
Швейцарская атака на «хакеров»
