Галия Ибрагимова
Консультант ПИР-Центра,
Кандидат политических наук Университета мировой экономики и дипломатии (Ташкент, Узбекистан)

16 июля 2014 г.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ПОВЕСТКЕ ДНЯ ШОС: НА ПУТИ К САММИТУ 2015 Г. В УФЕ

Сегодня аксиома о том, что использование информационно-коммуникационных технологий (ИКТ) оказывает самое серьезное влияние на стратегическую безопасность, экономическую и социально-политическую стабильность общества и государства, находит все больше зримых подтверждений на региональном уровне.

Военно-политическое противостояние на Ближнем Востоке сопровождается активным информационным противоборством и кампаниями политически мотивированных кибератак. События вокруг Украины также показывают, что информационные технологии, активно используются сторонами конфликта для подавления противника, нанесения ущерба его экономике, и в то же время для формирования и продвижения выгодной для себя версии событий на международном уровне. Достаточно вспомнить любой международно-политический кризис или военный конфликт последнего времени, чтобы убедиться, что информационное противоборство в интернете и атаки на информационную инфраструктуру стали их неотемлемым и немаловажным аспектом, а точнее – самостоятельным измерением конфликта.

Однако спектр угроз в области использования ИКТ не ограничен политически мотивированными кампаниями, равно как и последние не сводятся к DDoS-атакам и информационным кампаниям. Продвинутые вредоносные программы выводят из строя банковские системы и атакуют АСУ ТП нефтегазовых предпреятий и даже объектов атомной энергетики. Кибермошенничество

становится заурядным способом нелегального заработка во всех регионах мира, кибершпионаж в Сети делает доступными государственные секреты. «Дело Сноудена» стало убедительной иллюстрацией того, что электронный шпионаж за политическими лидерами, гигантами частного сектора и обычными гражданами давно систематической практикой работы спецслужб, проводимой в глобальном масштабе[1].

Таким образом, члены международного сообщества сегодня поставлены в условия, когда с одной стороны стимулирование ИТ-сектора и курс получение дивидендов от глобального и трансграничного взаимодействия в сфере ИКТ являются безоговорочным императивом для экономичекого развития и поддержания своей конкурентоспообсности. С другой же стороны, лица, принимающие решения, вынуждены все время быть начеку, чтобы не допустить использования современных информационных технологий для оказания днструктивного воздействия на государственную целостность, стабильность и национальную безопасность. Успешное противодействие таким угрозам невозможно на уровне отдельно взятой страны и требует активного внешнего сотрудничества, даже в условиях, когда отсутствует стопроцентное доверие к партнерам.

Государства Шанхайской организации сотрудничества (ШОС) не менее других участников глобальных процессов обеспокоены событиями, происходящими в сопредельных регионах и находящих прямое или косвенное отражение в киберпространстве. Страны ШОС сами неоднократно испытывали на себе последствия использования ИКТ в деструктивных целях. DDoS-атаки, взлом корпоративных и государственных сетей при помощи вредоносного кода, кибершпионаж и кибермошенничество - с этими явлениями столкнулось за последнее время каждое государство, входящее в Организацию.

Проблематика кибербезопасности – а точнее говоря, международной информационной безопасности (МИБ), – давно заняла одно из центальных мест из центральных мест в повестке дня ШОС. Участники организации еще в 2006 г. на саммите в Шанхае одними из первых в рамках международной организации приняли Заявление глав государств-членов ШОС по международной информационной безопасности. В документе выражалась озабоченность «использованием ИКТ в целях, наносящих ущерб безопасности человека, общества и государства». Приоритетной целью выражалось намерение государств скоординировано принимать меры для реагирования на угрозы безопасности в информационной сфере. В ходе последующих мероприятий ШОС принимались новые документы, регулирующие поведение государств в информационном простарнстве и ответственное использование ИКТ, но намерение действовать, полагаясь на единые меры доверия между странами объединения оставалось неизменным. .

Острота проблем обеспечения МИБ подчеркивалась в так называемой Екатеринбургской декларации ШОС, принятой государствами-членами в ходе саммита организации в Екатеринбурге 15-16 июня 2009 г[2]. Помимо декларации, в ходе саммита был также подписан основополагающий документ, который определил формат, цели и принципы сотрудничества стран Организации в области МИБ – Соглашение между правительствами государств-членов

Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. Соглашение стало первым документом подобного рода в мировой практике и, кроме того, также заложило общую терминологическую и концептуальную базу под подход ШОС, зафиксировов общее понимание таких базовых понятий как «разработка и применение информационного оружия, подготовка и ведение информационной войны», «информационный терроризм», «информационная преступность» и др.

В 2011 г. четыре страны-участницы ШОС (Россия, Китай, Узбекистан, Таджикистан). пошли еще дальше – на глобальный уровень, – представили в ООН свое видение проблем, связанных с МИБ, в разработанных и направленных письмом Генеральному Секретарю ООН Правил поведения государств в области обеспечение МИБ. Наконец, на саммите ШОС в Бишкеке в сентября 2013 г. внимание участников также было сфокусировано на вопросах МИБ и кибербезопасности. В ходе встречи главы государств приняли решение «стимулировать построение мирного, безопасного, справедливого и открытого информационного пространства, основываясь на принципах уважения государственного суверенитета и невмешательства во внутренние дела других стран». Это решение нашло отражение в Бишкекской декларации организации, принятой по итогам встречи[3].

Помимо ежегодных саммитов ШОС в рамках организации проводится значительное количество рабочих встреч, конференций, семинаров и других мероприятий с участием всех вовлеченных и заинтересованных сторон по вопросам обеспечения различных аспектов информационной безопасности.

В 2015 г. очередной саммит ШОС будет принимать Россия. Саммит пройдет в городе Уфа. В преддверии подготовки к саммиту можно предположить, что проблематика МИБ вновь окажется в числе приоритетных. В связи с этим возникает интерес не только к специфике проблем в области использования ИКТ, которые Россия вынесет на повестку обсуждений организации, но и к тому, насколько доверительными за годы существования организации, стали отношениями между е участниками, чтобы противостоять этим угрозам и вызовам и говорить об эффективности принимаемых совместных мер.

Государства-члены ШОС – Китай, Россия, Казахстан, Киргизия, Таджикистан и Узбекистан – географически близкие соседи. Несмотря на понимание важности многостороннего сотрудничества в рамках организации, процессы внутри- и внешнеполитического развития, культурно-ценностные ориентиры, а также значимость каждого субъекта организации в системе международных отношений различны. Отсюда, острота проблем кибербезопасности и информационной безопасности воспринимается государствами ШОС нескольк по-разному. Это, в свою очередь, влияет на эффективность реализации совместных инициатив в области использования ИКТ в контексте межлународной безпасности.

Например, Китай, выражая крайнюю обеспокоенность резко участившимися хакерскими атаками на стратегические национальные объекты и призывая в числе других государств-участников ШОС к совместным ответным правовым мерам противодействия угрозам, тем не менее, по оценкам спецслужб США, по-

прежнему возглавляет список государств, где власти сами попустительствуют подобным атакам, направленным против объектов в других странах[4]. Подобная двойственность в поведении КНР как крупнейшего в ШОС игрока на рынке ИКТ и, наряду с Россией, обладателя наиболее внушительного киберпотенциала, не может не вызывать опасения у других членов ШОС – государств Центральной Азии. Несмотря на демонстрируемое желание совместно противостоять киберугрозами, пока ситуация не в полной мере способствует укреплению мер доверия между странами ШОС и их качественной реализации. *Геополитическая подозрительность*, которая по-прежнему имеет место внутри ШОС, возрастает в связи с возникающими в информационном пространстве и киберпространстве, а также анонимными атаками, чье авторство не удается достоверно определить.

Что касается подходов государств Центральной Азии к развитию информационного пространства, то позитивным моментом следует считать то, что за последние годы представление о киберугрозах и их влиянии на национальную безопасность в регионе значительно расширились и углубились. Центральноазиатские республики вышли за рамки трактовки информационного пространства сугубо как арены, где ведется информационное противоборство между идеологическими противниками с целью подрыва политической стабильности в стране или регионе. Внедрение и расширение использования ИКТ и прежде всего интернет-коммуникации в различных инфраструктурных проектах, в сфере государственных услуг, в банковской и социальной сферах, в культуре и образовании привели к осознанию, что не только политическая, но и экономическая, энергетическая, инфраструктурная сферы – зависят от бесперебойного функционирования информационных систем. Результатам стал рост государственного внимания к вопросам обеспечения безопасности, устойчивости и защищенности информационных систем.

В государствах Центральной Азии в последнее время участились DDoS-атаки на правительственные сайты, сайты СМИ и другие информационные ресурсы в сети. По данным *Kaspersky Security Network*, Казахстан 85% атак через интернет в Центральной Азии, по сравнению с 8% в Узбекистане, 4% в Кыргызстане, 2% в Туркменистане и 1% в Таджикистане[5]. В этих условиях участники информационного рынка вынуждены активно реагировать на эти угрозы, последствия которых создают уже серьезные риски для безопасного мфункционирования стратегических объектов. Приходит все более четкое понимание необходимости не только очерчивать концептуальные рамки своих подходов, но и принимать конкретные технические меры по обеспечению безопасности информационных систем и сетей на региональном уровне.

Киберинциденты и атаки на информационные системы, с которыми сталкивались правительства центральноазиатских республик, по большей части носили характер кибермошенничества и или имели иные криминальные мотивы. Политическая мотивировка, которая традиционно приписывается кибератакам в Эстонии в 2007 г. или в Грузии в 2008 г., в Средней Азии до сих пор скорее отсутствовала[6]. Но по мере активного освоения как преступными элементами, так и акторами-посредниками информационного пространства государств Центральной Азии риски крупных кибератак с политической подоплекой растут. С еще большей уверенностью можно повторить этот прогноз в отношении кампаний информационного противодорства в интернете в условиях

возрастающей внутриполитической напряженности в Средней Азии. Одной из ее причин служит приближающаяся, пусть и в неясном временном горизонте, смена элит в двух наиболее крупных государствах региона – Узбекистане и Казахстане.

Таким образом, достижение единого понимания специфики развития информационного пространства и адекватное реагирование на киберугрозы становится центральной темой для всех государств членов ШОС, особенно в преддверии саммита ШОС в Уфе.

Государствам-членам ШОС важно осознать, что развитие информационного пространства и обеспечение безопасности от его угроз не зависит от государственных границ и национальных правовых рамок. Соответственно попытки государства в одиночку противостоять кибератам изначально подвержены неудаче. Только на основе совместных мер, многостороннего и регионального сотрудничества по проблематике киберугроз можно попытаться противостоять им. Отсюда, укрепление мер доверия и механизмов сотрудничества в области развития кибертехнологий между государствами членами ШОС становится основой для решения многих проблем в киберсфере. Такое сотрудничество способно привести к снижению деструктивного воздействия кибертехнологий на политическое, социально-экономическое, культурное развитие каждого государства члена ШОС и всей организации в целом.

Выработка совместных мер по предотвращению киберугроз способна нивелировать дефицит доверия государств ШОС друг к другу в вопросах, связанных с развитием информационного пространства и начать постоянное системное взаимодействие для борьбы с киберугрозами в реальном времени.

Россия и Китай – государства ШОС, наиболее активно вовлеченные в процессы развития глобального киберпространства, имеют возможность подключать Центральную Азию к более широкому и глубокому обсуждению проблем сфере ИКТ и принятию скоординированных мер по противодействию киберугрозам. Такой шаг не только повысит информированность внутри республик региона об актуальных проблемах в сфере МИБ, но и приведет к принятию совместных инициатив и мер, их поддержке и лоббированию на глобальном уровне.

Для практической реализации инициатив в сфере ипользования ИКТ в контексте международной безопасности в рамках Организации, целесообразно разработать единую стратегию обеспечения информационной безопасности и МИБ государств ШОС на ближайшие десять лет, и оформить ее в единый документ, обладающий юридической силой внутри самой Организации. В такой стратегии могли бы быть прописаны принципы открытости, доверительности и коллегиальности в работе государств участников организации по обеспечению МИБ. Такие принципы должны четко отражать заинтересованность государств ШОС сообща на региональном уровне работать над преодолением проблем в сфере использования ИКТ, а не придерживаться сугубо внутринациональных и односторонних подходов.

Значимая часть стратегии могла бы быть посвящена развитию и детализации общего терминологического аппарата стран ШОС в сфере МИБ, фундамент которого был заложен Екатеринбургским соглашением 2009 г. Особого внимания заслуживают вопросы, связанным с классификацией критической информационной инфраструктуры. Более того, региональный диалог на уровне ШОС мог бы служить «пробной площадки» для выработки общего, консенсусного понимания таких сложных и чувствительных проблем, как интерпретация применения к информационному пространству существующих норм международного права, включая Устав ООН и резолюции Генеральной Ассамблеи ООН, а также Гаагских и Женевских конвенций, составляющих фундамент международного гуманитарного права.

В документе также может быть предусмотрено создание постоянного рабочего аппарата ШОС, занятого вопросами МИБ и защиты информационных систем. Такой аппарат в формате Рабочей группы или отдела Секретариата ШОС мог бы вести свою деятельность по постоянной круглогодичной основе, обеспечивая организационную базу для таких совместных инициатив, как, например, CERT ШОС, и одновремеенно выступая площадкой для обмена специализированными экспертными мнениями между представителями стран Организации.

В 2006 г. в рамках ШОС уже создавалась Группа взаимодействия по нейтрализации киберугроз, которая, однако, представляла собой достаточно узкое по составу объединение специалистов и включала лишь представителей спецслужбы Региональной антитеррористической структуры ШОС[7]. В условиях активного вовлечения в киберпроцессы современности не только государств, но и частного бизнеса, гражданского общества, отдельных лиц представляется не совсем адекватным современным киберугроза. Важно, чтобы в рабочую группу по противостоянию киберугрозам входили не только спецслужбы, но и представители бизнеса, гражданского общества, отдельные специалисты и структуры, непосредственно занимающие вопросами борьбы с трансграничной киберпреступностью.

Деятельность такой рабочей группы по кибербезопасности могла бы вестись на базе единого Центра реагирования на киберугрозы (по сути, региональный CERT). Такой центр мог бы быть создан на базе структур ШОС или РАТС ШОС. Не исключено, что рабочая группа ШОС и центр ШОС по кибербезопасности мог бы работать на базе уже существующих структур или органов ШОС, специализирующихся на вопросах безопасности[8].

В качестве еще одной меры противодействия угрозам в области использования ИКТ могли бы стать ежегодные учения по кибербезопасности ШОС по аналогии с киберучениями, проводимыми в рамках ОДКБ «ПРОКСИ»[9]. Объединение навыков и совместная отработка практик как спецслужб, так и гражданских специалистов стран «шанхайской пятерки» в условиях, приближенных к реальным кибератакам, имеют все шансы стать ценной базой для наработки доверия и общего опыта в этой сфере.

Однако сложно ожидать, все меры и механизмы противодействия киберугрозам заработают на полную силу, если внутри стран ШОС не будет сформирован кластер высококвалифицированных специалистов – технической и

гуманитарной направленности – в МИБ и кибербезопасности. Развитие потенциала молодых специалистов в области ИКТ, разработка и реализация совместных образовательных программ, стажировок и принятие стандартов в области кибербезопасности между странами ШОС имело бы смысл сделать серьезным приоритетом Организации в деле противодействия современным вызовам и угрозам в области использования ИКТ.

В процессе выработки государствами участниками ШОС единой стратегии в области обеспечения МИБ вероятно и желательно вовлечение в диалог с другими дружественными региональными и международными форматами. Интерес к разработке мер доверия в сфере использования ИКТ и механизмов борьбы с трансграничной киберпреступностью проявляют страны АСЕАН, которые географически соседствуют с государствам ШОС. В перспективе ШОС могли бы расширять сотрудничество и с другими структурами на евразийском пространстве – СНГ, ОДКБ, ОБСЕ и др. Такое кросс-региональное взаимодйетвие способно обогатить практики входящих в эти структуры стран и способствовать рапространению успешного опыта в части, например, наработки мер доверия в киберпространстве.

Если в преддверии саммита ШОС в 2015 г. в Уфе государства-члены ШОС достигнут должного уровня взаимного доверия по ключевым вопросам информационной безопасности и кибербезопасности, и сумеют конвертировать этот капитал доверия в конкретные соглашения, практики совместных учений, работы и обмена данными, то позитивные последствия этого прогресса проявят себя далеко за предеами ШОС в силу трансграничности киберпространства. Но в оставшееся до саммита время на достижение такого результата нужно напряженно работать, развивая имеющиеся успехи.

---

[1] См., например: Интерфакс. Сюжет: Дело Сноудена. 11.06.2014, http://www.interfax.ru/story.asp?id=25 (последнее посещение 15 июля 2014 г.).

2 Екатеринбургская декларация глав государств – членов Шанхайской организации сотрудничества. 16 июня 2009 года. Официальный сайт Президента России. http://archive.kremlin.ru/text/docs/2009/06/217868.shtml (последнее посещение 15 июля 2014 г.).

[3] Главы стран ШОС подписали «Бишкекскую декларацию». Информационное агентство Regnum. 13 сентября 2009 г. http://www.regnum.ru/news/polit/1707374.html#ixzz37AVNjLl9 (последнее посещение 15 июля 2014 г.).

[4] Китаю предъявили киберобвинения. Газета Коммерсантъ. 21.05.2014. http://www.kommersant.ru/doc/2475664 (последнее посещение 15 июля 2014 г.).

[5]Аналитический обзор по Центральной Азии. Выуск №10июнь 2013. http://mason.gmu.edu/~emcglinc/Ru_CAP_Policy_Brief_10_June_2013.pdf (последнее посещение 15 июля 2014 г.).

[6] Там же.

[7] Спецслужбы ШОС решили бороться с киберугрозами. РИА Новости. 28.03.2014. http://ria.ru/world/20140328/1001453359.html (последнее посещение 15 июля 2014 г.).

[8] Шанхайская организация сотрудничества накануне саммита в Бишкеке: основные задачи момента. Сайт журнала «Международная жизнь», 22 мая 2013, http://lang.interaffairs.ru/index.php/ru/glavnaya/eksklyuziv/item/22-shankhajskaya-organizatsiya-sotrudnichestva-nakanune-sammita-v-bishkeke-osnovnye-zadachi-momenta (последнее посещение 15 июля 2014 г.).

[9] ОДКБ проводит операцию против киберпреступности. РИА Новости. 18.03.2010, http://ria.ru/defense_safety/20100318/215077305.html (последнее посещение 15 июля 2014 г.).