Второй сет мер укрепления доверия ОБСЕ в области кибербезопасности: что нового?

Александра Куликова, менеджер по взаимодействию с партнерами в Восточной Европе и Центральной Азии корпорации ICANN

В марте 2016 г. был опубликован согласованный в феврале второй перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий[1]. Он дополнил предыдущий перечень, состоящий из 11 предлагаемых мер, еще пятью пунктами. Новый сет отражает продолжающуюся тенденцию различных объединений государств к выработке механизмов, поддерживающих применение правил поведения государств в киберпространстве. В нем также угадываются противоречия, которые будут по-прежнему вставать на пути реализации согласованных мер.

О мерах доверия ОБСЕ

Первоначальный перечень мер укрепления доверия был принят в 2013 г., что стало первым международным (юридически не обязующим) соглашением по применению мер доверия в киберпространстве во избежание конфликтных ситуаций. Он состоит из 11 пунктов, отражающих намерение стран

[1] PC.DEC/1202. Решение № 1202. Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий. 1092-е пленарное заседание PC Journal No. 1092, пункт 1 повестки дня. 10 марта 2016. // URL: http://www.osce.org/ru/pc/228521?download=true

максимально прозрачно воплощать свои национальные киберстратегии, выработать эффективные механизмы, чтобы обмениваться оперативной информацией для предотвращения киберинцидентов и конфликтов с применением средств ИКТ.

Первый документ о мерах доверия в киберпространстве стал результатом долгих переговоров между странами, а принятый консенсусный пакет можно охарактеризовать как достаточно мягкий и неконкретный. Но это именно тот «общий знаменатель», который был возможен для стран-участниц в 2013 году. Пункты, о которых договорились участники ОБСЕ, отражают стремление государств научиться доверять друг другу в условиях значительного дефицита доверия, который с 2013 года только усугубился. Первый сет описывает меры транспарентности, обмен информацией, использование каналов государственных ведомств, а также групп оперативного реагирования для того, чтобы иметь возможность оперативно сообщать друг другу о каких-либо инцидентах, обмениваться лучшими практиками и т. д. Для того, чтобы поддерживать диалог вокруг этих мер доверия, была создана так называемая неформальная рабочая группа (Informal working group), которая должна собираться как минимум три раза в год для обсуждения имплементации этих мер и работы над расширением первоначального перечня.

Поскольку опыт работы над согласованием первого перечня показал, насколько велики могут быть разночтения различных сторон, предполагалось сфокусировать второй перечень на более конкретных мерах, особенно в отношении критической инфраструктуры (КИ). В будущем, третий сет должен сформулировать меры поддержания стабильности в киберпространстве, опираясь на работу, проведенную Группой правительственных экспертов по международной информационной безопасности (ГПЭ) ООН, и дополняя ее.

Согласование второго перечня шло непросто, и его содержанию, как и содержанию первого, также не хватает гранулярности. Тем не менее в нем нашли отражение рекомендации по развитию механизмов государственно-частного партнерства для реализации уже согласованных мер укрепления доверия. Предложено расширить список тех мероприятий, которые проводят государства для обмена информацией и лучшими практиками — в пункте 14 указано, что «государства-участники будут <…> способствовать государственно-частному партнерству и развивать механизмы обмена передовых опытом реагирования на общие вызовы безопасности, связанные с использованием ИКТ». Также в пункте 12 рекомендовано «приглашать к участию и задействовать в такой деятельности представителей частного сектора, научных кругов, центров передового опыта и гражданского общества».

Так, в январе 2016 года, примерно за два месяца до публикации второго перечня, Германия, к которой в 2016 г. перешло председательство в ОБСЕ, первым же своим мероприятием в этой роли провела конференцию по вопросам безопасности при использовании ИКТ[2]. При этом к обсуждению вопросов кибербезопасности помимо представителей правительств были привлечены и другие заинтересованные стороны: бизнес, общественные и экспертные организации, в том числе, технические экспертные организации, которые могли бы дать квалифицированную оценку появляющимся предложениям. Приглашенным на конференцию представителям заинтересованных сторон предложили обсудить дальнейшие перспективы работы в рамках ОБСЕ как по разработке и внедрению мер доверия, так и прочим инициативам, включая нормы поведения государств. Традиционно эти вопросы находятся в политико-военной плоскости, однако на мероприятии они были рассмотрены и в гуманитарном измерении — в свете обязательств стран по защите прав человека, — а также в экономическом измерении, где свои предложения вносили представители частного сектора.

Как известно, российская сторона с осторожностью относится к мультистейкхолдерному подходу в вопросах безопасности, последовательно подчеркивая ответственность и примат полномочий госорганов в области ее обеспечения при использовании ИКТ. Все же расширение круга привлеченных заинтересованных лиц, имеющих возможность внести вклад в это обсуждение и будущие рекомендации (например, на дополнительных экспертных площадках), могло бы позволить квалифицированно оценить, как согласованные меры доверия могут дать конкретный результат в разнообразных национальных контекстах стран-участниц.

Отдельный пункт в новом сете посвящен критически важной инфраструктуре. Как и в докладе Группы правительственных экспертов ООН, рекомендовано повышать безопасность критической национальной и транснациональной инфраструктуры, сформулировать ее национальную классификацию, категоризировать инциденты, поддерживать дальнейший диалог о гармонизации усилий именно в отношении КИ. Можно было бы ожидать отдельные положения по конкретным структурам: например, банковской, ядерной, о глобальной системе уникальных идентификаторов интернета. Но объекты КИ управляются и регулируются по-разному в различных странах, к тому же именно их стратегический характер ожидаемо препятствует открытости обмена информацией даже между самыми близкими партнерами.

Важно, что в тексте второго перечня неоднократно подчеркивается, что рекомендованные меры укрепления доверия являются добровольными и

[2] Berlin OSCE Cyber conference looks to reduce the risk of conflict stemming from Information and Communication Technologies. – OSCE. 20 January 2016 // URL: http://www.osce.org/cio/217426

должны осуществляться в соответствии с национальным законодательством. То есть, их реализация будет определяться интересами национальной безопасности и исходя из принципа национального суверенитета. Это, с одной стороны, сохраняет за государствами достаточно большую свободу в степени открытости, гранулярности добровольно предоставляемых данных в ходе сотрудничества. С другой стороны, несколько нивелирует эффективность этих мер: она прямо пропорциональна, собственно, тому исходному доверию, которое необходимо для эффективности совместных усилий по предотвращению киберинцидентов. При этом реальная оперативная работа, осуществляемая на уровне правоохранительных органов и технических сообществ осуществляется в параллельной плоскости, независимо от (не)заключаемых соглашений на высшем уровне.

И все же, работа над мерами укрепления доверия в рамках ОБСЕ и за ее пределами видится полезным и важным элементом более широкой экосистемы мер поддержания стабильности, мира и безопасности.

Обсуждение правил поведения в киберпространстве

Выработка норм поведения в информационном пространстве в настоящее время обсуждается сразу на нескольких международных площадках: в ГПЭ ООН, в БРИКС, в Шанхайской организации сотрудничества и др. Участвует в процессе обсуждения и частный сектор — так, свои собственные нормы для государств в 2014 г. предложила корпорация Microsoft[3]. Эти нормы, прежде всего, направлены на то, чтобы не допустить использования программных продуктов для целей злоумышленников.

О нормах поведения часто говорят, как об одном из подходов к поддержанию стабильности в киберпространстве, и эта область неразрывно связана с темой мер укрепления доверия. Можно сказать, что без укрепления доверия поддержание стабильности, в общем-то, невозможно. В докладе ГПЭ ООН 2015 г.[4] секция, посвященная таким мерам, прописана достаточно подробно. ОБСЕ также будет опираться на работу ГПЭ в разработке и третьего сета мер укрепления доверия. В Уфимской декларации БРИКС в 2015 г. тоже есть

[3] Paul Nicholas. Six Proposed Norms to Reduce Conflict in Cyberspace. - Microsoft Cyber Trust Blog. January 20, 2015 // URL: https://blogs.microsoft.com/cybertrust/2015/01/20/six-proposed-norms/

[4] A/70/174. Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Записка Генерального секретаря. Семидесятая сессия. Пункт 93 предварительной повестки дня. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». 22 июля 2015. // URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

отдельный пассаж по мерам укрепления доверия[5], а в обновленном предложении ШОС «Правила поведения в области обеспечения международной информационной безопасности» в пункте 10 предлагается «развивать меры укрепления доверия в целях повышения предсказуемости и снижения вероятности недопонимания, а также риска возникновения конфликта». В первоначальной версии «Правил…» этого пункта не было.

Таким образом, очевидно, что курс на нормотворчество и на укрепление доверия между государствами будет пересекаться и дальше, потому что без доверия невозможно говорить ни о каких нормах поведения не только в формате государственных актов, но и на других уровнях. В вопросе о доверии между государственными акторами и корпоративным сектором будут действовать те же механизмы, которые тоже полезно обсуждать. Например, когда речь заходит о глобальной инфраструктуре интернета, где важнейшую роль играют частные операторы этих инфраструктур.

Интересно, что просматривается попытка расширить круг стейкхолдеров, которые участвуют как в обсуждении мер укрепления доверия, так и норм поведения в киберпространстве[6]. В целом две дискуссии пересекаются очень плотно. Работа в ОБСЕ в определенном смысле инспирирована процессом ГПЭ ООН и наоборот, что способствует взаимообогащению решений, обмену идей. Вероятно, в следующей Группе правительственных экспертов по международной информационной безопасности, как и в ОБСЕ, еще более подробно будет рассматриваться вопрос о нормах поведения в отношении безопасности КИ. Страны ОБСЕ, в свою очередь, видят перспективной дискуссию о мерах поддержания стабильности в киберпространстве, и на этом будет сфокусирован третий сет мер доверия ОБСЕ.

[5] VII саммит БРИКС. Уфимская декларация. Уфа, Российская Федерация, 9 июля 2015. Неофициальный перевод // URL: http://infobrics.org/wp-content/uploads/2015/07/VII_sammit_BRIKS_Ufimskaya_deklaratsiya.pdf

[6] Netherlands and Estonia to set up cyber platform. – Government of the Netherlands. 16-11-2015 // URL: https://www.government.nl/latest/news/2015/11/16/netherlands-and-estonia-to-set-up-cyber-platform