МЕРЫ ДОВЕРИЯ И БЕЗОПАСНОСТИ В СФЕРЕ ИКТ И ВОПРОСЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Обсуждение в ОБСЕ мер доверия и безопасности в киберпространстве началось с создания при организации в 2009 г. по решению № 1039 профильной Неформальной рабочей группы открытого характера[1]. Эта группа была, как считается, создана по инициативе представителя США при ОБСЕ посла Иэна Келли. Выработка новых мер доверия идет как раз в рамках, а точнее, *под эгидой* этой неофициальной группы, поскольку фактически работа на каждый момент ведется не более чем в пяти-шести столицах. И хотя решения этой группы не являются обязывающими, их реализацию нельзя не учитывать при оценке уровня информационной безопасности государств — членов Организации.

Говоря о мерах укрепления доверия и безопасности, в первую очередь стоит определиться, о чем идет речь.

Впервые как международно-правовой инструмент меры доверия появились в Соглашении между СССР и США о мерах по уменьшению опасности возникновения ядерной войны 1971 г.[2]. В последующем эта форма межгосударственного сотрудничества была закреплена в Соглашении о предотвращении ядерной войны 1973 г.[3].

Реально работающим механизмом меры доверия стали после подписания Заключительного акта Совещания по безопасности и сотрудничеству в Европе 1975 г.[4] и включения его в практику работы СБСЕ, а затем и ОБСЕ. Хельсинкский акт предусматривал, в частности, предварительное уведомление о крупных военных учениях, обмен наблюдателями на военных учениях и предварительное уведомление о крупных передвижениях войск.

Меры доверия, зафиксированные в Заключительном акте, были усовершенствованы документом Стокгольмской конференции 1986 г. по мерам укрепления доверия и безопасности и разоружению в Европе[5]. Этот документ с однозначностью показал, что страны — участницы конференции видят меры доверия и безопасности не только как конкретные действия, но и относят их не иначе как к военной сфере.

Таким образом, надо четко осознавать, что есть меры доверия, которые относятся, в основном, к сфере культуры, гуманитарному измерению, а есть меры доверия и безопасности — именно в такой формулировке — которые относятся к военной и только к военной сфере и нацелены на снижение уровня военного проти-

востояния государств. Их нельзя смешивать, хотя не следует и противопоставлять. Именно в дополнении мер доверия и безопасности мерами доверия можно найти комплексное решения проблемы обеспечения мирного сосуществования. Как подчеркивается в Документе Стокгольмской конференции, первостепенную важность имеет соблюдение десяти обозначенных в Хельсинкском Заключительном акте принципов, которыми государства-участники будут руководствоваться во взаимных отношениях. Такой подход, кстати, мог бы послужить хорошей базой для международной конвенции по обеспечению международной информационной безопасности, особенно если дополнить указанные принципы правилами поведения в информационной сфере.

Россия всегда в своей политике контроля над вооружениями приветствовала принятие мер доверия и безопасности как важного механизма обеспечения международного мира и снижения уровня военных угроз.

Этот подход в целом распространяется и на сферу международной информационной безопасности. В частности, в представленной на Встрече высоких представителей, курирующих вопросы безопасности (Екатеринбург, 21–22 сентября 2011 г.), концепции Конвенции об обеспечении международной информационной безопасности прямо указано на то, что каждое государство-участник должно стремиться к укреплению мер доверия и безопасности в области военного использования информационного пространства, к которым относятся:

1) обмен национальными концепциями обеспечения безопасности в информационном пространстве;

2) оперативный обмен информацией о кризисных событиях и угрозах в информационном пространстве и принимаемых мерах в отношении их урегулирования и нейтрализации;

3) консультации по вопросам деятельности в информационном пространстве, которая может вызывать озабоченность государств-участников, и сотрудничество в отношении урегулирования конфликтных ситуаций военного характера[6].

Однако такой принципиальный подход не означает, что Россия, как и любая другая страна, должна в любых ситуациях соглашаться на принятие на себя обязательств по любым мерам доверия безотносительно их соответствия национальным интересам и интересам безопасности, в том числе с учетом наших внешнеполитических обязательств и интересов наших партнеров.

Аналогичный подход исповедуется и в США. Анализ документов и выступлений американских и натовских экспертов показывает, что те выделяют три группы мероприятий, которые могли бы быть отнесены к мерам доверия:

- меры транспарентности, которые позволяют сделать взаимодействие более предсказуемым;
- межгосударственные консультации, которые направлены на совместное обсуждение угроз и выработку рекомендаций по борьбе с ними;
- меры добровольного ограничения деятельности, то есть добровольное принятие странами на себя конкретных обязательств относительно отказа от тех или иных действий, которые могут рассматриваться как недружественные или даже опасные.

Вместе с тем существует и другой подход к принятию мер доверия и безопасности как формы международных отношений государств в сфере безопасности. Многие эксперты считают, что принятие подобных мер эффективно, только когда такое решение принимается на уровне ООН и распространяется на все страны. В противном случае вступает в дело юридический принцип всеобщности, делающий соглашение, реализующее эти меры, недействительным в отношениях с третьими странами, а следовательно, сохраняющий для заключивших соглашение стран угрозы, против которых направлены принятые меры, а значит, и уровень их обороноспособности, что, в свою очередь, требует наращивания военного потенциала. Кроме того, установление доверительных отношений между потенциальными противниками невозможно в принципе, а обязательные при заключении соответствующего соглашения даже незначительные уступки могут повлечь за собой в дальнейшем отход от принципиальных позиций. Меры доверия и безопасности, в том числе и в информационной сфере, по своей природе затрагивают весьма чувствительные вопросы, требующие всестороннего рассмотрения в контексте государственной и общественной безопасности.

Формально существующие международные документы не ограничивают список вооружений, к действиям с применением которых могут быть отнесены меры доверия и безопасности. Поэтому появление в начале нынешнего десятилетия в ОБСЕ идеи распространить этот механизм на информационное оружие, в качестве которого могут рассматриваться информационно-коммуникационные технологии, нельзя считать неестественным шагом[7].

Все, что происходит в рамках ОБСЕ в вопросах международной информационной безопасности, относится к сфере мер доверия и безопасности, т. е. все это по определению следует относить к военной сфере. Однако этот факт почему-то часто упускают из виду. А зря. Из сказанного следует фактическое признание государствами ОБСЕ наличия в современных международных отношениях войн в информационном пространстве (с использованием информационных средств воздействия[8]) и желания вести их как бы более гуманно, *доверяя* друг другу.

В упомянутом выше документе Стокгольмской конференции для реализации мер доверия и безопасности в качестве обязательного предусмотрен механизм верификации. Это означает, что он должен быть прописан и в соответствующем соглашении, распространяющем меры доверия и безопасности на другие, не предусмотренные Итоговым документом, сферы. Если обратиться к мерам доверия, пакет которых был принят Постоянным советом ОБСЕ в 2013 г.[9], то в Решении № 1106 таковых вроде бы нет. Можно сослаться на то, что во введенном решением перечне неоднократно подчеркивается добровольный характер принятых мер. Однако следует внимательнее рассмотреть следующий за перечнем мер раздел Решения № 1106 Постоянного совета (PC. БЕС/1106 3 декабря 2013 г.) ОБСЕ под названием *Практические соображения*. В соответствии с ним «государству-участнику, желающему получить разъяснения по поводу того или иного индивидуального сообщения, предлагается делать это на заседаниях Комитета по безопасности и его неофициальной рабочей группы, учрежденной Решением № 1039 Постоянного совета[10], либо путем вступления в прямой диалог с представившим его государством с использованием устоявшихся механизмов для контактов, включая список адресов электронной почты и дискуссионный форум POLIS».

По сути это основа механизма контроля исполнения означенных в Перечне мер, то есть механизма верификации, пусть и находящегося в зачаточном состоянии.

Что может означать на практике это положение, ведь, как говорят сторонники принятых мер, они все равно остаются добровольными и государство вправе само решать, что отвечать и отвечать ли на эти вопросы? Представим себе, что представителя государства *поднимут* на Комитете по безопасности, в зале, полном по этому случаю журналистов, и спросят: «Почему данную информацию ваша страна представила так, а не по-другому? Ведь говорят, что есть другая информация, отличная от этой. Объясните, пожалуйста, этот факт». Действительно ли добровольным является представление информации, если представителю государства предложат публично ответить? А может ли он *добровольно* не отвечать на этот вопрос в присутствии представителей прессы? Или, скорее, эта добровольность относительная? И будет ли при освещении этого диалога учитываться политический фактор? Ведь до сих пор при отсутствии каких-либо доказательств Россию обвиняют в информационных атаках на Эстонию, имевших (или нет — доказательств не представлено) место в 2007 г. Какие вопросы были бы заданы Постоянному представителю России при ОБСЕ, если бы к тому времени уже были бы приняты решения, аналогичные документу № 1106? И принял ли бы кто-нибудь его объяснения и подтверждающие их аргументы? Известно, что нельзя доказать отсутствие чего-либо, всегда остается предположение, что-де *слишком хорошо спрятали*. Даже при отсутствии презумпции невиновности, что мы нередко вынуждены бываем отмечать в практике международных отношений.

В итоговом докладе четвертой группы правительственных экспертов (ГПЭ) ООН по международной информационной безопасности, работавшей в 2014–2015 г. на основании резолюции 68 сессии ГА ООН *Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности*[11], также содержится перечень мер доверия, по своему содержанию во многом пересекающийся с венскими. Вместе с тем их изложение, особенно в пунктах 17 и 18, содержит модальности, позволяющие ставить вопрос о декларировании Группой необходимости механизма контроля исполнения. Поэтому вся дискуссия, в основном, проходит не вокруг того, что включать в меры доверия, нужны они или не нужны, а вокруг того, как реализовывать эти меры и где заканчивается доверие и начинается верификация.

Последний пакет мер укрепления доверия в сфере ИКТ, одобренный в феврале этого года в рамках ОБСЕ[12], затрагивает, вероятно, самый скользкий момент — критическую инфраструктуру. Что означает обмен информацией об инцидентах на объектах критической инфраструктуры? В моем понимании, это предоставление сведений о средствах, которыми была осуществлена акция, о мерах, которые были приняты для защиты объекта, о результате применения средств защиты на объекте, о последствиях атаки для функционирования объекта. Однако как ответы на эти вопросы, крайне чувствительные для национальной безопасности, соотносятся с интересами безопасности государств, на территории которых находятся или которым принадлежат упомянутые инфраструктуры? Потенциальные противники, спецслужбы и военные структуры были бы готовы дорого заплатить за такую информацию. Гораздо больше она заинтересовала бы террористические организации. Представьте, что было бы, если бы террористы получили доступ

к информации о том, как защищены критические инфраструктуры и какие средства нападения наиболее *успешны*.

Аналогичные предложения (создать единый или распределенный банк данных, систему свободного обмена информацией и т. п.) не раз звучали (почему-то, в основном, от американцев) и на других переговорных площадках в рамках нераспространенческой и антитеррористической тематик. Однако они практически никогда не находили поддержки экспертов. Им, в отличие от политиков, изначально было понятно, что решение вопросов ограничения доступа к подобным сведениям и предотвращения их *нецелевого* использования будет куда сложнее, чем поддержание традиционных форм сотрудничества.

Вопрос о включении пункта о критических инфраструктурах в пакеты мер доверия — один из самых сложных, и подходить к нему нужно осмотрительно, разобравшись, в первую очередь, с проблемами национальной безопасности.

Подводя итог, хочу еще раз обратить внимание на то, что меры доверия и безопасности в любой области предотвращения конфликтов и обеспечения мирного сосуществования государств не могут быть мерами принуждения и должны основываться на учете национальных интересов, суверенитета и равноправия всех государств.

Александр Федоров,
член Экспертного совета ПИР-Центра

Примечания

1 В практике ОБСЕ *открытый характер* означает отсутствие фиксации состава группы и проведение ее заседаний вне зависимости от наличия кворума. Решение теоретически может быть принято и одним председателем, хотя это, конечно, вырожденный случай.

2 Соглашение о мерах по уменьшению опасности возникновения ядерной войны между Союзом Советских Социалистических Республик и Соединенными Штатами Америки. Вашингтон, 30 сентября 1971 г., http://old.nasledie.ru/politvne/18_9/article.php?art=26 (последнее посещение — 1 июня 2016 г.)

3 Соглашение между Союзом Советских Социалистических Республик и Соединенными Штатами Америки о предотвращении ядерной войны. Вашингтон, 22 июня 1973 г., http://old.nasledie.ru/politvne/18_24/18_24_1/article.php?art=8 (последнее посещение — 1 июня 2016 г.)

4 Совещание по безопасности и сотрудничеству в Европе. Заключительный акт. Хельсинки, 1 августа 1975 г., https://www.osce.org/ru/mc/39505?download=true (последнее посещение — 1 июня 2016 г.)

5 Документ Стокгольмской конференции по мерам укрепления доверия и безопасности и разоружению в Европе, созванной согласно соответствующим положениям Итогового документа Мадридской встречи Совещания по безопасности и сотрудничеству в Европе. Стокгольм, 1986 г., http://www.osce.org/ru/fsc/41242?download=true (последнее посещение — 1 июня 2016 г.).

6 Конвенция об обеспечении международной информационной безопасности (концепция), http://www.scrf.gov.ru/documents/6/112.html (последнее посещение — 1 июня 2016 г.).

7 Вопрос возможности применения информационно-коммуникационных технологий в качестве оружия, конечно, спорный, как минимум в лингвистическом смысле, но в политических кругах такая трактовка признается правомерной. Хотя какой ущерб может нанести технология как таковая, понять и объяснить непросто. Лично мне встречать рациональное объяснение или хотя бы конкретные примеры такого не приходилось.

8 Поскольку понятие *оружие* не определено, видимо, предпочтительным следует признать использование этого термина вместо получившего распространения термина *информационное оружие*.

Что под ним понимать, можно найти в выпущенной ПИР-Центром под моей и В. Н. Цыгичко редакцией еще в 2001 г. монографии *Информационные вызовы международной и национальной безопасности*, http://www.pircenter.org/media/content/files/9/13464042510.pdf (последнее посещение — 1 июня 2016 г.).

9 PC. DEC/1106. Решение № 1106. Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий. Организация по безопасности и сотрудничеству в Европе, Постоянный совет, 975-е пленарное заседание. 3 декабря 2013 г. PC Journal No.975, пункт 1 повестки дня, http://www.osce.org/ru/pc/109648?download=true (последнее посещение — 1 июня 2016 г.).

10 PC. DEC/1039. Решение № 1039. Разработка мер укрепления доверия с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий. Организация по безопасности и сотрудничеству в Европе, Постоянный совет, 909-е пленарное заседание. 26 апреля 2012 г. PC Journal No.909, пункт 2 повестки дня, http://www.osce.org/ru/pc/90634?download=true (последнее посещение — 1 июня 2016 г.).

11 A/70/174. Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Записка Генерального секретаря. 22 июля 2015 г., http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (последнее посещение — 1 июня 2016 г.).

12 PC. DEC/1202. Решение № 1202. Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий. Организация по безопасности и сотрудничеству в Европе, Постоянный совет, 1092-е пленарное заседание. 10 марта 2016 г. PC Journal No.1092, пункт 1 повестки дня, http://www.osce.org/ru/pc/228521?download=true (последнее посещение — 1 июня 2016 г.).