РОССИЙСКАЯ АССОЦИАЦИЯ МЕЖДУНАРОДНЫХ ИССЛЕДОВАНИЙ

Материалы VII Конвента РАМИ

Секция № 13

Безопасность: традиционные и новые формы военной активности

Плотников Владислав Александрович, к.полит.н., заместитель декана Факультета международных отношений Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации

Международная информационная безопасность во внешнеполитической стратегии России

В настоящее время стало очевидным, что прозрачность государственных границ для информационных потоков ведет к возникновению принципиально новой ситуации для обеспечения национальной безопасности. Отсутствие комплексной всесторонней защищенности информационного пространства государства может привести к значительному ограничению его суверенитета, и существенному ослаблению позиций страны на мировой арене.

В качестве одного из ключевых аспектов противостояния в рассматриваемой сфере выступает информационная война. При этом информационная война рассматривается не как обособленные действия, а как интеграция всех форм и способов вооруженной борьбы, при которой происходит значительное сокращение привлекаемых сил и средств за счет повышения информационных возможностей.

Ее суть заключается в том, что войска достигают информационного превосходства, под которым понимается как поступление информации в большем количестве, так и более высокая степень доступа к ней более мелких звеньев системы и, как следствие, более глубокое понимание ситуации на поле боя. Это становится возможным в результате доступа географически разбросанных войск к единой информационной системе. При этом синхронизация их действий достигается уже не за счет централизованного управления, а за счет своевременной реакции этих войск на изменения обстановки.

Для лишения возможного противника заблаговременно накопленной информации, а также для минимизации наносимого в результате ведения разведки ущерба уже в мирное время должно осуществляться противодействие видовой и радиоэлектронной разведкам иностранных государств, которая ведется космическими и воздушными разведывательными системами и системами двойного назначения.

Закон Российской Федерации «О безопасности» предусматривает деление национальной безопасности на следующие виды: государственную, экономическую,

общественную, оборонную, информационную, экологическую и иные (ст. 13). В качестве угроз в информационной сфере в рамках Концепции национальной безопасности России 2000 г. рассматривается следующее: «Серьезную опасность представляют собой стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним»[1].

На смену этому документу пришел новый, отражающий перемены, происходящие в международной системе и внутри страны. В 2009 г. была принята Стратегия национальной безопасности России до 2020 г., которая отразила ключевые взгляды, в том числе на основные проблемы в информационной сфере: «Угрозы информационной безопасности в ходе реализации настоящей Стратегии предотвращаются за счёт совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации, повышения уровня защищённости корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности»[2].

Довольно важным фактором было признано «…развития общей гуманитарной и информационно-телекоммуникационной среды на пространстве государств – участников Содружества Независимых Государств и в сопредельных регионах»[3]. Информационные аспекты отмечены уже в каждой из сфер безопасности в качестве одних из ключевых.

В то же время на данный момент все еще действует Доктрина информационной безопасности 2000 г.[4], оформленная в качестве надстройки вслед за принятием базовой Концепции национальной безопасности, однако не получившая достаточной юридической силы. Дело в том, что Доктрина информационной безопасности, несмотря на достаточно развернутую программу действий по обеспечению безопасности страны в этой области, не получила возможности проведения ее в жизнь.

Наконец, в 2010 г. вышел новый федеральный закон «О безопасности», который вновь если не расширил, то четко очертил вместе с другими сферами довольно четко и ясно и информационную область безопасности. Безусловно, эта законодательная инициатива была вызвана к жизни быстроменяющимися условиями, особенно внешнеполитического характера.

Для нашей страны очевидным направлением действий по обеспечению собственной информационной безопасности выступает выведение этого вопроса на международный уровень, где основу составляют наиболее востребованные в отечественной внешней политике международные структуры – Содружество Независимых Государств, Шанхайская организация сотрудничества и Организация Объединенных Наций.

---

[1] Концепция национальной безопасности Российской Федерации // Совет безопасности Российской Федерации. – 2000 г. – Url.: http://www.scrf.gov.ru/documents/1.html.

[2] Стратегия национальной безопасности Российской Федерации до 2020 года // Президент России. – 13 мая 2009 г. – Url.: http://xn--d1abbgf6aiiy.xn--p1ai/ref_notes/424.

[3] Там же.

[4] Доктрина информационной безопасности // Российская газета. – Url.: http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm.

Приоритет остается, естественно за работой с ближайшими соседями на той территории, где уровень доверия максимально высок, ведь современная Россия достигла репутации весьма надежного исполнителя своих международных обязательств. Поэтому первые инициативы отрабатывались на странах СНГ, еще в 2006 г. была принята Концепция формирования информационного пространства Содружества Независимых Государств, в которой недостаточно развернуто, но четко прописана необходимость коллективного обеспечения информационной безопасности[5]. Сам документ послужил лишь поводом к интенсификации работы в этом направлении на многостороннем уровне и подтолкнул к запуску следующего этапа.

Дальнейшие события привели к тому, что именно Евразийский регион и Российская Федерация выступили в качестве инициаторов перехода на новый уровень международного взаимодействия в области информационной безопасности. Через десять лет после запуска процесса по объединению усилий в области информационной политики в СНГ, страны, увязывавшие свое участие в многосторонних межгосударственных институтах с повышением доверия в области границ смогли подключить дополнительные ресурсы[6]. Все это выразилось в формировании в 2006 г. группы экспертов Шанхайской организации сотрудничества по международной информационной безопасности. Как и в случае с определением ключевых аспектов терроризма, ШОС в плане информационной безопасности задала тон глобальному сообществу[7]. С первых дней своей работы Группа экспертов привлекла внимание Генеральной Ассамблеи ООН. Этот шаг сблизил позиции по ключевым понятиям не только среди стран-членов ШОС, но и среди экспертов, представляющих отдаленные регионы.

Следующим этапом стало представление в 2010 г. контактной группой из пятнадцати стран Генеральному секретарю ООН доклад, в котором впервые на столь высоком уровне говорилось о необходимости выработки общих подходов в борьбе с киберугрозами, и признавалось, что угрозы эти могут исходить не только от преступников и террористов, но и от государств. В сентябре 2011 г. этот этап дополнился новым шагом, выразившимся в обнародовании двух программных документов – «Правилах поведения в области обеспечения международной безопасности» и проекте конвенции ООН «Об обеспечении международной информационной безопасности».

Последнее заседание контактной группы прошло 8 июня 2012 г. в Санкт-Петербурге, а этот год может стать завершающим для принятия нового международного документа, способного очертить основные категории (информационная война «информационная инфраструктура, информационное оружие, информационное пространство), принципы и методы обеспечения информационной безопасности и другие важнейшие аспекты, выработанные при непосредственном участии нашей страны и способные соизмерить и внести вклад в стабилизирующую роль в информационные аспекты современной системы международных отношений.

---

[5] Косов Ю.В., Торопыгин А.В. Проблема безопасности государств - членов евразийского экономического сообщества // Управленческое консультирование. Актуальные проблемы государственного и муниципального управления. 2005. № 2. С. 100-107.

[6] Косов Ю.В., Плотников В.А. На пути к новому партнерству в Евразии // Управленческое консультирование. 2012. № 1. С. 223-226.

[7] Кучерявый М.М., Плотников В.А. Региональная модель формирования информационного общества (на примере Содружества Независимых Государств) // Евразийская интеграция: экономика, право, политика. – 2012. №11. С. 118-119.