Секция «Международное право»

Международно-правовое регулирование противодействия кибертерроризму

Научный руководитель – Евстифеева Екатерина Владимировна

Гусайниева Патимат Ибрагимовна
Студент (специалист)
Саратовская государственная юридическая академия, Саратов, Россия
E-mail: patimat.gusaynieva.96@mail.ru

В современных условиях наблюдается растущая зависимость государственных органов власти, промышленных предприятий, общественных организаций и индивидуальных пользователей от информационных и коммуникационных технологий в плане осуществления своих функций, ведения дел, обмена информацией, предоставления государственных услуг. В результате усиливающейся взаимосвязанности информационные системы и сети подвергаются все более многочисленным и разнообразным угрозам, которые создают новые проблемы в плане безопасности, в том числе национальной и международной[5]. Современные террористы используют новые информационные технологии, вследствие чего появился новый вид терроризма, а именно кибертерроризм. Новый вид характеризуется также осуществлением своей деятельности посредством и внутри глобальной сети Интернет. За последние пять лет выросло количество кибератак, проводимых на территории РФ. На 2015 г. было зафиксировано наибольшее количество, за этот год атакам подверглось более 600 сайтов российских компаний и государственных органов, блокировалась работа этих сайтов, а затем размещали на них пропагандистские материалы. Главной же целью был вывод из строя общественно важных сайтов, сбой деятельности организаций и критически важных объектов инфраструктуры, запугивание и распространение паники и хаоса среди населения Российской Федерации[2]. Одновременно с понятием огромной ценности информации возникает потребность и в ее защите. Со временем социальные преобразования привели к необходимости законодательного регулирования новых общественных отношений. Необходимо отграничивать понятие «информационно-технологическим терроризм», т.е. кибертерроризм, от понятия «информационно-психологический терроризм». В то время, как противодействие информационно-психологическому терроризму более или менее законодательно урегулирован, противодействие кибертерроризму имеет достаточно слабое регулирование. Еще в 1930 г. на III Международной конференции по унификации уголовного законодательства в Брюсселе были перечислены действия, относящиеся к возможным угрозам информационно-технологического терроризма, которые в совокупности представляют собой вывод из строя критически важных объектов инфраструктуры, следовательно можно говорить о возможных колоссальных ущербах. Помимо всего прочего, определяющим в разработке нормативной базы является то, что киберпростанство не имеет границ, в связи с этим кибертерроризм можно считать международной угрозой. Для эффективного противодействия данной угрозе необходимо, как отметил Президент России В.В. Путин, выступая на расширенном заседании коллегии ФСБ России в 2012 г: «. . . сформировать единую систему обнаружения, предупреждения и отражения компьютерных атак на информационные ресурсы». 23 ноября 2001 года начато подписание Европейской конвенции о киберпреступности странами-членами СЕ, ее ратификация[1]. Нормы данной конвенции, в случае ее ратификации многими странами будут унифицированы, что позволит создать единую систему борьбы с киберпреступностью и мониторинг компьютерных преступлений. Несмотря на значительные достоинства Конвенции, существуют некоторые проблемные аспекты, так п. b ст. 32 Конвенции содержит положения,

которые могут трактоваться как способные причинить ущерб суверенитету и безопасности государств-участников конвенции и правам их граждан. Также необходимо отметить, что в данном соглашении не участвуют такие государства, как Российская Федерация, Китай, страны Латинской Америки, что серьезно снижает возможность по созданию эффективного механизма сотрудничества по борьбе с киберпреступностью. Следует отметить, что Российская Федерация два года готовилась к подписанию данного документа[4]. Президента РФ в Распоряжении от 15.11.2005 г. №557-рп «О подписании Конвенции о киберпреступности» отмечает, что Российская Федерация определится в вопросе о своем участии в Конвенции при условии возможного пересмотра положений данного пункта, чего сделано не было. Россия 22 сентября 2011 года представила странам-участникам ООН концепцию Конвенции «Об обеспечении международной информационной безопасности. С критикой документа выступили США и Великобритания, опасающиеся распространения цензуры, так же концепция не получила поддержки со стороны ЕС, так как их взгляды на сферу действия подобного документа существенно отличались от, предложенной Российской Федерацией, сферы действия. Координатор «Центра безопасного интернета в России» Урвана Парфентьева отметила, что, формулируя претензии к проекту конвенции, США учитывают слабость отсылок в ее тексте к общепризнанным гражданским и политическим правам человека, что дает им возможность говорить о возможной легитимизации цензуры. Но положения Международного пакта о гражданских и политических правах данная конвенция не отменяет. Эти права и свободы действуют независимо от конвенции. Индия и Китай, в свою очередь, поддержали концепцию, предложенную Российской Федерацией. С Китаем даже был подписан проект резолюции Генассамблеи ООН по общим правилам поведения в интернете - «мягкий» вариант конвенции[3]. Для борьбы с кибертерроризмом имеются, в том числе, подписанные и функционирующие международные правовые акты. 16 июня 2009 г. в Екатеринбурге было подписано Соглашение между правительствами государств-членов ШОС «О сотрудничестве в области обеспечения международной информационной безопасности», вступившее в законную силу 2 июня 2011 года. Данное Соглашение углубляет и развивает положения антитеррористической концепции, которая была утверждена 5 июля 2005 г. и в которой борьба с кибертерроризмом рассматривается в качестве одного из основных направлений сотрудничества государств-членов ШОС. Также существует межправительственное соглашение с Республикой Куба о сотрудничестве в области обеспечения международной информационной безопасности и российско-кубинского заявления о неразмещении первыми оружия в космосе, регулирующая отношения по борьбе с кибертерроризмом. Всего Россия провела 5 межведомственных консультаций по международной информационной безопасности с Германией, Кубой, Францией, Южной Кореей и Японией. Безусловно можно говорить о том, что это не может обеспечить в полной мере эффективное противодействие кибертерроризму. Спецпредставитель Президента РФ по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских отмечал: «Россия уже несколько раз планировали провести консультации с Канадой. . . , но, увы, эти планы каждый раз срывались по разным причинам, в последний раз из-за санкций»[6].

Источники и литература

1) Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования// Правовые вопросы связи. 2004. № 2. С.17-25.

2) Зверянская Л. П. Проблема кибертерроризма с точки зрения российского общества// ИСОМ. 2015. №6-2.

3) Матвеева А.Понятие свободы не абсолютно //Газета.ru: интернет-издание. 2012.

4) Мороз Н. О. Международно-правовое сотрудничество в борьбе с киберпреступностью в рамках Европейского союза и Совета Европы // Науч. тр. Акад. упр. при Президенте Республики Беларусь.2009. Вып.11,ч.2. С.86-95.

5) Пахарева Е. Н. Влияние кибертерроризма на молодежную среду: особенности и тенденции развития // Ученые записки РГС.2011. №2.

6) www.mid.ru (Министерство иностранных дел Российской Федерации).