

Секция «Мировая политика»

Информационный терроризм как новая угроза международной безопасности

Мансуров Абдулмалик Зиявдинович

Студент

*Российская правовая академия МЮ РФ, Северо-Кавказский филиал, Юридический факультет, Махачкала, Россия
E-mail: 55555malik55555@mail.ru*

Информационный терроризм как новая угроза международной безопасности

Мансуров Абдулмалик Зиявдинович

Студент Северо-Кавказского филиала Российской правовой академии МЮ РФ, Махачкала, Россия

Стремительное развитие компьютерных технологий и международных компьютерных сетей приводит к соблазну использовать достижения информационных технологий и средств манипулирования общественным сознанием для экспансии во всех сферах жизнедеятельности общества и государства: в экономике, политике, науке, культуре, обеспечении национальной и международной безопасности, применяя не ограниченный никакими положениями международного права абсолютно новый вид информационного оружия – информационный терроризм.

Информационный терроризм как современное социально-политическое явление представляет серьезную угрозу международной безопасности общества и государства в целом. Несомненно, что применение террористами новейших информационных технологий сильно расширяет возможности совершения противоправных действий, позволяет привлекать к себе всеобщее внимание и держать людей в постоянном страхе.

Переход человечества на новый информационно-технический уровень развития выдвинул основополагающий принцип деятельности государств в информационном пространстве – принцип мирного использования единого международного информационного пространства, но при этом информационное пространство используется не только в мирных целях, но и становится лакомым кусочком для террористов, которые для достижения своих целей принимают на вооружение новые информационные средства воздействия и технологии информационной войны. Они превратили классическую террористическую деятельность в кибертерроризм–терроризм информационной эры.

Наиболее актуальна проблема распространения информационного терроризма в республиках СКФО. Усиление государством силовых мер для борьбы с преступлениями террористической направленности, зачастую, не приводят к желаемым результатам. В связи с этим остро стоит вопрос о необходимости усиления мер информационной безопасности населения с целью предупреждения совершения таких преступлений.

Отличительной чертой информационного терроризма является его дешевизна и сложность обнаружения. Интернет предоставляет свободный доступ, массовость аудитории, анонимность связи, ограниченность возможностей контроля и цензуры, быстроту передачи информации, все это, несомненно, благоприятствуют деятельности террористических организаций. Анонимность, обеспечиваемая Интернетом, позволяет террористу

стать невидимым и, как следствие, практически неуязвимым и ничем (в первую очередь, жизнью) не рискующим при проведении преступной акции. Положение усугубляется тем, что преступления в информационной сфере, в число которых входит и кибертерроризм, влекут за собой наказание существенно меньшее, чем за осуществление "традиционных" террористических актов. Например, Уголовный кодекс РФ за неправомерный доступ к компьютерной информации, если это деяние повлекло наступление тяжких последствий предусматривает наказание, не превышающее семи лет лишения свободы. Для сравнения, в США законы карают несанкционированное проникновение в компьютерные сети заключением сроком до 20 лет [1]. Кроме того, в США функционируют так называемые кибервойска, деятельность которых специально направлена на борьбу с такими формами проявления терроризма.

На расширенном заседании коллегии ФСБ, посвященном итогам работы службы за 2012 год, Президент РФ В.В. Путин отметил, что при нейтрализации разного рода экстремистских структур нужно действовать максимально решительно, блокировать попытки радикалов использовать для своей пропаганды возможности современных информационных технологий, ресурсы интернета, социальных сетей.

В целях противодействия использованию информационного пространства в террористических целях мы предлагаем усилить меры наказания за использование информационного пространства в террористических целях и признать необходимость совместных решительных действий.

Анализ существующих международных политико-правовых документов в области информационной безопасности позволяет предположить отсутствие достаточной международной правовой законодательной базы, позволяющей эффективно решать проблемы информационного терроризма, которые в настоящее время охватили мировое сообщество [2].

Стратегия международного сотрудничества в сфере информационной безопасности в настоящее время должна разрабатываться на глобальном уровне.

Базовыми элементами для развития такого международного сотрудничества должны стать:

- определение характеристик возникающих угроз, связанных с информационным терроризмом, и достижение общего понимания потенциальных угроз;
- выработка меры предотвращения использования информационных технологий и средств, в террористических и других преступных целях;
- выработка адекватных мер по обнаружению потенциальных угроз и противодействию им;
- определение формы принуждения для прекращения актов информационного терроризма;
- выработка защитных механизмов и практических методов снижения угроз и уязвимости информационных систем и сетей;
- создание системы международного мониторинга для отслеживания угроз информационного терроризма и механизма контроля выполнения режима международной информационной безопасности;
- совершенствование межведомственного взаимодействия силовых структур по координации действий в сфере борьбы с информационным терроризмом;

- совершенствование нормативно правовой базы, регулиующую антитеррористическую деятельность.

Естественно, что каждая страна сама должна разрабатывать свою систему мер по снижению специфических угроз информационного терроризма, однако внесенные нами выше положения могут быть положены в основу международной программы по защите от информационного терроризма.

Российская Федерация, как одна из самых уязвимых государств от преступлений террористической направленности, должна взять на вооружение все наиболее эффективные и рациональные средства и методы борьбы с информационным терроризмом с целью защиты основ конституционного строя страны, защиты интересов личности, общества и государства от противоправных посягательств.

Литература

1. Газизов Р.Р. Информационный терроризм // Материалы Международной научно-практической конференции «Проблемы противодействия преступности в современных условиях». 16-17 октября 2003г. Часть I. Уфа, 2003.
2. Горбенко А.Н. Правовое регулирование в сфере информационного противоборства // Информационное право. 2008. №3. С. 32-37.