Секция «Мировая политика»

Кибертерроризм как угроза международной безопасности.

Бидная Ксения Васильевна
Студент
С(А)ФУ им. М.В.Ломоносова, Управления и регионологии, Архангельск, Россия
E-mail: kseniya_bidnaya@mail.ru

Технический прогресс и развитие общества в конце XX века открыли миру немыслимые до этого перспективы и возможности, которые к началу XXI века обусловили вступление современной цивилизации в абсолютно новую эпоху. Она была охарактеризована американским социологом и футурологом Элвином Тоффлером как информационное общество, где главным фактором общественного развития является производство и использование информации. Но такие коренные изменения, безусловно, влекут за собой и новые сложности, социальные конфликты и глобальные проблемы, столкнуться с которыми человечеству придется в XXI веке.

Встраивание компьютеров в управление объектами государственной и частной инфраструктуры являются причиной все большего распространения и возрастания значимости кибертерроризма в мире [10], поскольку эти элементы считаются наиболее уязвимыми перед террористической атакой.

Кибертерроризм по своим масштабам превосходит другие виды террора, он не имеет национальных границ, террористические акты могут осуществляться из абсолютно любой точки земного шара, в киберпространстве сегодня не действуют договоры и соглашения, принятые международным сообществом [2]. Помимо этого, на сегодняшний день затруднено обнаружение террористов в киберпространстве, поскольку они действуют через один или цепочку подставных компьютеров, затрудняющих идентификацию и определение их местоположения.

По данным Государственного агентства США отвечающего за безопасность гражданских компьютерных сетей - US-CERT, в 2006 году было зарегистрировано 2172 кибератаки, в 2008 году - 54488, а в 2009 почти 10 000 [1]. Очевидно, что столь стремительное развитие данной проблемы требует не менее стремительного поиска путей ее решения мировым сообществом, однако большинство современных политиков считают, что каждое государство должно выстраивать собственную систему защиты от кибернападения, что является в корне неправильным подходом к решению проблемы глобального характера и обуславливает задержку в принятии международных документов правового регулирования киберпространства, а также планомерных программ международного сотрудничества государств с целью предотвращения и борьбы с актами кибертерроризма.

На сегодняшний день наиболее полноценным документом в борьбе с кибертерроризмом можно считать Стратегию министерства обороны США в сфере киберпространства [8]. Но и она не может быть взята на вооружение всеми странами мира, поскольку в ней четко просматривается лоббирование интересов самих США и попытки ограничения и цензурирования Интернета.

Проблема кибертерроризма носит глобальный характер, ее решение должно быть найдено при участии всех стран мира, поэтому общими являются и методы борьбы с киберугрозой. Исходя из особенностей кибертерроризма, можно выделить 3 основных

направления борьбы: создание законодательной базы, наличие специально обученных кадров, наличие необходимых передовых технических средств.

Как и большинство стран мира, где была создана развитая система компьютерного управления, Россия оказывается в зоне риска перед угрозой террористической кибератаки. Ключевой особенностью Российской Федерации в киберпространстве является с одной стороны, ее нормативная и концептуальная незащищенность от киберугроз и с другой, крупная неорганизованная хакерская сеть. Именно благодаря этому, в рейтинге кибермогущества Россия занимает только 14 позицию, суммарно получив 31,7 баллов [9]. Интересно, что при этом некоторые зарубежные и отечественные политики и журналисты присваивают России роль первооткрывателя кибервойны [4, 6].

Главной проблемой кибербезопасности России является отсутствие государственного плана защиты страны. Причем на сегодня даже не ведутся какие-либо разработки в этой области. Существующая Концепция противодействия терроризму в Российской Федерации 2009 г. [3] не уделяет должного внимания угрозе террора из киберпространства, сосредоточившись на более «классическом» понимании терроризма и его видам. Доктрина информационной безопасности РФ 2000 г. [7] также относительно устарела и в основном посвящена защите информации в телекоммуникационным пространстве, без подробного рассмотрения киберпространства. Представляется очевидным, что этих мер недостаточно для гарантированной защиты страны, а также возможности ведения ею кибервойны. Отсутствие полноценного плана защиты страны от киберугрозы в современном компьютеризированном мире представляют серьезную опасность для успешного развития нашей страны. Необходимо создание нормативно-правового акта направленного на защиту интересов страны в киберпространстве и предусматривающего ряд конкретных мер по противодействию кибертерроризму. Необходимо создать специальное военное подразделение, а также комитет, с целью предотвращения кибератак, разработки защиты для объектов государственной и частной инфраструктуры, а также, при необходимости, подготовки равноценного ответа на кибернападение со стороны других государств. На сегодня подобные подразделения уже создаются в некоторых странах [5]. Помимо этого специфика киберпространства предполагает наличие технически современного оборудования для его защиты.

Проведенное исследование показало, что стремительно растущая компьютеризация всех сфер жизни общества, в том числе и стратегически важных, а также ежегодно растущие темпы совершенствования форм и методов негативного кибервоздействия и нарастание угрозы кибератаки, выводят значение кибертерроризма в современном мире на новый уровень. Универсальный характер кибертерроризма ведет к сплочению стран, ведь, киберпространство – свободное поле, без государственных границ и рамок, где все страны находятся под угрозой кибератаки, поэтому и защита должна быть выработана совместно.

Литература

1. Белянинов К. Если завтра кибервойна // Огонек. 2010. 19. С. 28-27.

2. Возженникова А.В. Международный терроризм: борьба за геополитическое господство. М.: РАГС. 2005.

3. Концепция противодействия терроризму в Российской Федерации // Российская газета. 2009, 20 октября. 5022. С.4.

4. A cyber risk to the U.S. // The Washington Post. 2012, February 13. P. 5

5. Lewis L. Chinese cyberwarriors build shield around military secrets // The Times. 2011, 27 May. P. 9

6. Mannes A., Hendler J. The first modern cyberwar? // The Guardian. 2008, 22 August. P. 7

7. Российская газета. Доктрина информационной безопасности РФ: http://www.rg.ru/oficial/d

8. Department of defense strategy for operating in cyberspace: http://www.defense.gov/news/d201

9. The Cyber Hub. Who is Leading the Race to Become a Cyber Superpower?: http://cyberhub.con

10. The Federal bureau of investigation. Issue of Intrusions into Government Computer Networks: http://www.fbi.gov/news/testimony/issue-of-intrusions-into-government-computer-networks

Слова благодарности

Хотелось бы выразить слова благодарности оргкомитету конференции "Ломоносов а именно Антону Алексееву, за своевременный ответ и помощь в оформлении тезисов через систему автоматического макетирования.