

Зяблов Денис Николаевич

ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТА ТЕРРОРИСТИЧЕСКИМИ ОРГАНИЗАЦИЯМИ В СОВРЕМЕННОМ МИРЕ

В данной статье автор характеризует содержание террористических сайтов, выясняет, кто является объектом информационного терроризма, почему именно Интернет является столь привлекательным для террористических организаций. Предлагаются меры по противодействию использованию террористическими группировками сети Интернет.

Адрес статьи: www.gramota.net/materials/3/2011/4-3/11.html

Источник

Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики

Тамбов: Грамота, 2011. № 4 (10): в 3-х ч. Ч. III. С. 42-45. ISSN 1997-292X.

Адрес журнала: www.gramota.net/editions/3.html

Содержание данного номера журнала: www.gramota.net/materials/3/2011/4-3/

© Издательство "Грамота"

Информацию о том, как опубликовать статью в журнале, можно получить на Интернет сайте издательства: www.gramota.net
Вопросы, связанные с публикациями научных материалов, редакция просит направлять на адрес: voprosy_hist@gramota.net

11. Стругацкие А. и Б. Обитаемый остров [Электронный ресурс]. URL: <http://lib.ru/STRUGACKIE/ostrow2.txt> (дата обращения: 17.04.2011).
12. Тюрин А. Боятся ли компьютеры адского пламени? [Электронный ресурс]. URL: http://fan.lib.ru/t/tjurin_a_w/text_0010.shtml (дата обращения: 17.04.2011).
13. Тюрин А. Каменный век [Электронный ресурс]. URL: http://fan.lib.ru/t/tjurin_a_w/tyurin-stoneage.shtml (дата обращения: 17.04.2011).
14. Тюрин А. Мы и цифровая жизнь [Электронный ресурс]. URL: http://fan.lib.ru/t/tjurin_a_w/tyurin_interview_hi_tech.shtml (дата обращения: 17.04.2011).
15. Тюрин А. О кибергуманизме [Электронный ресурс]. URL: http://fan.lib.ru/t/tjurin_a_w/tyurin-cyberhumanism.shtml (дата обращения: 17.04.2011).
16. Чекмаев С. Спамелла // Фантастика 2006: сб. Серия «Звездный лабиринт». М.: АСТ; АСТ-МОСКВА; ХРАНИТЕЛЬ, 2006. Вып. 2. С. 234-248.
17. Эллисон Х. У меня нет рта, чтобы кричать [Электронный ресурс]. URL: <http://readr.ru/harlan-ellison-u-menya-net-rta-chtobi-krichat.html> (дата обращения: 17.04.2011).

SCENARIOS OF PERSON AND TECHNICS COEXISTENCE IN LITERARY ALLOTOPIA

Artur Aleksandrovich Dydrov

Department of Philosophical Sciences
Chelyabinsk State Academy of Culture and Arts
diskoboll@mail.ru

The article is devoted to considering one of the topical problems of the end of the XXth – the beginning of the XXIst centuries – the problem of the coexistence of humans and technics generated by them. This problem has found expression not only in scientific works but also in a variety of art works - allotopias - which as a whole generated the trend of cyberpunk.

Key words and phrases: allotopia; technics; cyberpunk genre; tendency; future.

УДК 34

В данной статье автор характеризует содержание террористических сайтов, выясняет, кто является объектом информационного терроризма, почему именно Интернет является столь привлекательным для террористических организаций. Предлагаются меры по противодействию использованию террористическими группировками сети Интернет.

Ключевые слова и фразы: Интернет; терроризм; информационный терроризм; кибертеррористы; свободный доступ к Интернету; сайты террористического характера.

Денис Николаевич Зяблов

Кафедра «Информатизация правовой деятельности»
Тамбовский государственный технический университет
denis_zyablov@lantamail.ru

ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТА ТЕРРОРИСТИЧЕСКИМИ ОРГАНИЗАЦИЯМИ В СОВРЕМЕННОМ МИРЕ[©]

Современное общество – это общество информационное. Сейчас каждый человек может овладеть чуть ли не любой информацией и в огромном количестве. Казалось бы, люди достигли совершенства знания: доступно все, все можно узнать – надо только зайти в поисковые системы в Интернете. Главное, правильно ввести запрос. Но не всякое знание несет настоящее знание, и не всякая информация полезна. Информационная революция вместе со всеми преимуществами принесла и серьезные проблемы в сфере общественной безопасности. В первую очередь это касается распространения терроризма в Интернете. По данным Национального антитеррористического комитета РФ, в настоящее время в мире действует около 5 тысяч интернет-сайтов, активно используемых террористами. Число порталов, обслуживающих террористов и их сторонников, постоянно растет [9].

В статье предпринята попытка анализа использования террористическими организациями сети Интернет в своих преступных целях. В качестве постановки проблемы можно поставить следующие вопросы:

- 1) каково традиционное содержание террористических сайтов;
- 2) кто является объектом информационного терроризма;
- 3) почему именно Интернет является столь привлекательным для террористических организаций;
- 4) каковы методики и механизмы использования сети Интернет террористическими группировками.

Как правило, сайт содержит информацию об истории организации и ее действиях, детальный обзор социальных и политических истоков, отчет о наиболее заметных делах, биографию лидеров, основателей и героев, сведения о политических и идеологических целях, жесткую критику врагов и текущие новости.

Зачастую террористическая организация изображается как постоянно преследуемая: ее лидеры подвергаются попыткам убийства, последователи арестовываются, свобода выражения ограничивается. Такая тактика, изображающая организацию маленькой, слабой и преследуемой мощью сильного государства, рассчитана на привлечение «сочувствующих» последователей. Члены движения или организации представляются борцами за свободу, использующими насилие против их желания, потому что безжалостный враг ущемляет права и достоинство людей. Враг движения или организации – якобы настоящий террорист, множество сайтов настаивают: «Наше насилие ничтожно по сравнению с его агрессией». Это наиболее общий аргумент. Террористы перекладывают ответственность за насилие с себя на противника, который обвиняется в демонстрации зверства, жестокости и безнравственности.

Обратившись к одному из террористических сайтов, можно заметить, что внешне он вполне демократический, ориентирован на западный путь развития, который считает единственно правильным, предлагает строительство России на основе западных гуманистических ценностей с признанием нерушимости демократических прав и свобод, частной собственности и свободной рыночной экономики. Но в своей «Революционной программе» руководитель движения призывает к отделению Чечни от России, жестко критикует Правительство РФ, агитирует к борьбе с неверными и прочее. Подобных ресурсов много. И все они содержат ссылки на другие террористические организации [8].

Террористы используют открытость цивилизованного мира для реализации своих целей. Раньше им было труднее организовывать и исполнять террористические акты из-за расстояния и координации действий. Сейчас таких проблем нет. С помощью Интернета преступники могут согласовать время, место проведения терактов. Так, сервис *Google Maps* дает очень широкие возможности для всех пользователей Интернета без исключения, предоставляя в открытом доступе спутниковые снимки и карты любой местности. При террористической атаке в индийском городе Мумбаи использовался именно сервис *Google Maps*, благодаря подробностям, которые можно изучить с его помощью, террористы планировали свои действия. Поэтому калифорнийские конгрессмены предложили некий закон АВ-255, согласно которому в *Google Maps* нужно размывать изображение определенных областей, чтобы их нельзя было детально изучать. К таким объектам относятся школы, церкви, больницы и правительственные сооружения. Вместо них законодатели предлагают созерцать цветные размытые пятна. Нововведение не запрещает людям определять направление маршрутов, но вентиляционные отверстия и лифтовые шахты не должны отображаться на экране. Это правильный шаг в борьбе с терроризмом. Но не следует забывать, что и без предлагаемого *Google* сервиса достать карты интересующей местности в наше время не составляет труда. Со спутниковыми снимками немного сложнее, но и их при желании достать вполне возможно.

Страшнее всего то, что боевики размещают на сайтах руководства по изготовлению бомб, оружия, организации терактов и пр. Владельцы сайтов, которые вывешивают подобные инструкции, обычно избегают наказания, утверждая, что не они являются авторами руководств и что они не призывают использовать данную информацию на практике.

Террористы могут атаковать или проникнуть внутрь компьютерных систем различных учреждений. Последствия этого могут быть разнообразные: пострадать могут военные, разведывательные, медицинские службы, транспортные и финансовые системы и т.д. Потенциальные масштабы кибертерроризма ужасны, поскольку они могут внести хаос в действия не только государственных, но и коммерческих структур, парализовав, например, банковские операции [1].

Чтобы воздействовать на людей, террористы используют психологическую атаку, которая заключается в распространении угроз, направленных на то, чтобы посеять страх и ощущение беспомощности. Именно с этой целью распространялась, например, видеозапись убийства американского журналиста Дэниэла Перла лицами, захватившими его в плен. Террористы также могут начать психологические атаки посредством кибертерроризма, а точнее, создания опасений угрозы совершения таких действий. «Киберстрах» возникает из беспокойства об угрозе компьютерных нападений (например, падение самолетов, вывод из строя систем управления воздушным движением, сбой в системе национальной экономики путем нарушения компьютерных систем, регулирующих фондовые биржи и т.п.), которое усиливается настолько, что общество начинает верить, что атака случится.

Как и другие политические организации, террористические группы используют сеть для пополнения фондов. Демографические данные интернет-пользователей (получаемые, например, из личной информации, введенной в онлайн анкету или бланк заявки) позволяют террористам идентифицировать отношение аудитории к той или иной проблеме. С помощью сети руководители террористических сайтов осуществляют сбор денежных средств на поддержку преступных операций, на содержание боевиков.

Террористы используют в своих целях и рекламные возможности сети. Им очень выгодно придавать своим действиям гласность, не привлекая при этом телевидение, радио или печатные СМИ, что сделать гораздо сложнее. Делается это для запугивания потенциальных врагов. Чтобы привлечь сторонников, а главное молодежь, сайты террористических организаций часто выполняют функции интернет-магазинов: они предлагают купить флаги, футболки, плакаты, значки, аудио- и видеозаписи с их символикой [7].

Интернет стал благодатной почвой и для распространения слухов. Теракты, совершенные в Москве весной 2010 года, активно обсуждались в чатах, блогах и форумах: очевидцы или участники становились чуть

ли не «звездами», пытаясь поделиться пережитыми впечатлениями, порой приукрашивая свершившееся. В сети стали появляться слухи об организации теракта, его руководителях. Некоторые из них были очень далеки от реальности, тем не менее получали поддержку общественности.

Анализ содержания этих сайтов позволяет выделить три группы лиц, на которых в первую очередь ориентированы данные сайты:

- текущие и потенциальные сторонники;
- члены международной аудитории, непосредственно не вовлеченные в конфликт, но в некоторой степени заинтересованные в проблеме. Большинство сайтов имеют версии на нескольких языках. Для удобства иностранных посетителей сайты представляют основную информацию об организации с множеством второстепенных исторических обзорных материалов – материалов, с которыми сторонники организации, скорее всего, уже знакомы. Судя по содержанию многих сайтов, в потенциальную аудиторию включены также иностранные журналисты. Для озвучивания позиции организации в традиционных СМИ используются пресс-релизы на сайтах. Детальная второстепенная информация очень полезна для международных корреспондентов. Некоторые сайты направляют усилия на деморализацию противника, угрожая нападением и создавая чувство вины за мотивы и поведение неприятеля. Они также стремятся стимулировать общественные дебаты в государствах-врагах, повлиять на общественное мнение и ослабить поддержку обществом существующей власти;
- сочувствующие, для которых террористические сайты используют лозунги и выставляют на продажу значки, футболки, флаги, видеозаписи, аудиокассеты и т.п. Часто организация, заинтересованная в локальной поддержке в какой-либо местности, создает сайт на соответствующем языке, располагая на нем детальную информацию о действиях и внутренней политике организации, ее союзниках и врагах.

По своей природе Интернет во многих отношениях – идеальное поле деятельности террористических организаций. Прежде всего, имеются в виду предлагаемые глобальной сетью следующие возможности:

- свободный доступ;
- небольшие регулирование, цензура и другие формы государственного контроля или вовсе их отсутствие;
- потенциально огромная аудитория во всем мире;
- анонимность связи;
- быстрое движение информации;
- невысокая стоимость создания сайта и обслуживания присутствия в сети;
- мультимедийная среда: возможность комбинировать текст, графику, аудио и видео, возможность для пользователей загружать фильмы, песни, книги, постеры и т.д.;
- возможность охватить также аудиторию традиционных СМИ, которые все чаще используют Интернет как источник сообщений.

Указанные преимущества не остались незамеченными террористическими организациями, независимо от их политической ориентации. На сегодняшний день почти все активные террористические организации имеют веб-сайты, а многие поддерживают более одного сайта и используют несколько языков [1].

Эти организации находятся в разных точках земного шара. Причем отметим, что географическая категоризация иллюстрирует географическое разнообразие, но затеняет тот факт, что многие группы являются в действительности межнациональными и даже трансрегиональными по характеру.

Выделяют восемь различных, хотя и иногда частично совпадающих, способов использования сети Интернет террористами. Это – психологическая война; реклама и пропаганда; сбор данных; сбор средств; вербовка и мобилизация; создание сетей; распределение информации; планирование и координация.

Некоторые из них похожи на те, которыми использует глобальную сеть каждый пользователь (например, сбор информации). Другие напоминают использование средств популяризации традиционными политическими организациями (например, сбор средств и пропаганда). Третьи намного более необычны (например, отправка инструкций в закодированных сообщениях или зашифрованных файлах).

Таким образом, террористическое движение в Интернете – четко спланированное психологически направленное воздействие на население, и организуют его специально подготовленные люди, обладающие определенными знаниями. Именно они направляют «толпу», особенно воздействуя на тех, кто имеет несформировавшееся мировоззрение и кто не определился со своим предназначением в жизни [6].

Как бороться с терроризмом? Тем же методом – информированием. Террористы используют ложную информацию с целью вербовки. У мирного населения должно быть информирование с целью знания – что такое терроризм, как он проявляется в Интернете, какие сайты существуют, какова их цель, к чему приводит участие в подобных группировках и прочее. Знание равно оружию. Человека знающего и осведомленного не так просто сбить с пути.

В настоящее время существующие в Уголовном кодексе Российской Федерации статьи, предусматривающие ответственность за терроризм, не способны в полной мере охватить деятельность террористических организаций в сети Интернет, в связи с чем количество сайтов террористической направленности, а также связанной с этим информации в Интернете с каждым годом не убавляется, а лишь становится больше. Это позволяет террористическим организациям привлекать на свою сторону больше сторонников, распространяя нужную им информацию среди общества, а также получать необходимую информацию для совершения терактов.

Кроме того, с терроризмом надо бороться на мировом уровне – сотрудничать в области правовой взаимопомощи, обмена разведывательными данными. Необходимо принятие единых законов по борьбе с

преступностью в компьютерной сфере с тем, чтобы расследование преступлений и следствие по таким уголовным делам проводились бы независимо от национальных границ. Правоохранительным органам важно продолжать изучение и контроль террористических действий в Интернете, а также поиск мер по ограничению использования этой среды современными террористами.

Таким образом, противодействие использованию террористическими группировками сети Интернет является важной задачей не только правоохранительных органов, но и всего гражданского сообщества в целом. Представляется необходимым проводить активную антитеррористическую работу, в том числе и при использовании современных информационных технологий.

Список литературы

1. Вейманн Габриэль. Специальный доклад № 116 от 02.03.2005 [Электронный ресурс] / перевод Татьяны Тропиной. URL: http://www.crime-research.ru/analytics/Tropina_01 (дата обращения: 04.04.2011).
2. Галкин А. Ю. Состав террористического акта в рамках последних изменений статьи 205 Уголовного кодекса Российской Федерации // Исторические, философские, политические и юридические науки, культурология и искусствоведение: вопросы теории и практики. 2009. № 1. С. 28-30.
3. Матчанова З. И. Мотивация террористической деятельности: криминологический анализ // Там же. № 3. С. 114-116.
4. Слезин А. А. Государственная функция политического контроля: особенности правоприменительной практики // Вестник Тамбовского государственного технического университета. 2007. Т. 13. № 3. С. 821-825.
5. Слезин А. А. Политический контроль как функция государства // Юридический мир. 2007. № 1. С. 59-62.
6. Тимоти Л. Томас. Терроризм и Интернет: проблемы взаимодействия [Электронный ресурс] // Право и безопасность. 2001. № 1. URL: http://www.dpr.ru/pravo/pravo_1_9.htm (дата обращения: 04.04.2011).
7. <http://www.chekist.ru/article/2893>
8. <http://www.crime.vl.ru>
9. http://www.saferunet.ru/ruaos/stories/detail.php?SECTION_ID=136&ID=982

INTERNET USE BY TERRORIST ORGANIZATIONS IN MODERN WORLD

Denis Nikolaevich Zyablov

Department of Legal Activity Informatization

Tambov State Technical University

denis_zyablov@lantamail.ru

In the article the author characterizes terrorist sites content, finds out who is the object of information terrorism, why Internet is so attractive for terrorist organizations and suggests counteraction measures against Internet network use by terrorist groupings.

Key words and phrases: Internet; terrorism; information terrorism; cyber-terrorists; free access to Internet; sites of terrorist character.

УДК 34

В данной статье рассматривается проблема использования особенностей сети Интернет злоумышленниками в целях распространения в ней информации экстремистского характера. Автор пытается выявить основные направления борьбы с экстремизмом в Интернете.

Ключевые слова и фразы: экстремизм; Интернет; контроль за информацией; цензура в Интернете.

Денис Николаевич Зяблов

Кафедра «Информатизация правовой деятельности»

Тамбовский государственный технический университет

denis_zyablov@lantamail.ru

ПРОТИВОДЕЙСТВИЕ ПРОЯВЛЕНИЯМ ЭКСТРЕМИЗМА В СЕТИ ИНТЕРНЕТ®

Ежегодно повышается степень организованности экстремистов, для достижения своих целей активно укрепляющих международные связи, широко использующих информационные и телекоммуникационные технологии, в том числе Интернет. Федеральный список экстремистских материалов, публикуемый Минюстом России на сайте www.minjust.ru/ru/activity/nko/fedspisok/, постоянно пополняется и сегодня включает в себя 806 материалов, признанных судом экстремистскими, из которых 87 были опубликованы на интернет-сайтах. «Одним из основных внешних факторов, способствующих возникновению и распространению терроризма в Российской Федерации, является распространение идей терроризма и экстремизма через Интернет и средства массовой информации», – указано в Концепции противодействия терроризму в Российской Федерации, утвержденной Президентом Российской Федерации Д. А. Медведевым 5 октября 2009 г. Таким