ISSN 1998-4001

CAICAT POLICY

№11, қараша, 2012 ж.

CAЯCAT-POLICY
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЖУРНАЛ
ИЗДАЕТСЯ С 1995 ГОДА
ВЫХОДИТ ЕЖЕМЕСЯЧНО

Издание зарегистрировано Комитетом информации и архивов Министерства культуры и информации Республики Казахстан. Свидетельство о постановке на учет №10416-Ж от 20.10.2009 г.

Подписной индекс 75861

Собственник - ИП Ертурина Кульбаршин

Адрес редакции:
050012 г. Алматы
ул. Богенбай батыра, 86
Тел.: +7 727 291-90-28
+ 7 777 033-44-22

Подписано в печать 20.11.2012.
Формат 60x90 1/8
Печать офсетная.
Тираж 1000 экз.

№ 11 (205) //2012

ЧИТАЙТЕ В НОМЕРЕ

МАЗМҰНЫ СОДЕРЖАНИЕ

ГОСТЬ НОМЕРА

ЭКОНОМИКА

ПОЛИТИКА

ТРАНСПОРТ

СОЦИОЛОГИЯ

УВАЖАЕМЫЕ ЧИТАТЕЛИ!

Ежемесячный
информационно-аналитический
журнал «САЯСАТ-POLICY» и
ежеквартальный научно-теоретический
журнал «ЕВРАЗИЙСКОЕ СООБЩЕСТВО»,
утвержденные Комитетом по контролю
в сфере образования и науки
МОН РК для публикации статей
в области общественных наук:

- издаются с 1995 г. и 1997 г. соответственно;
- распространяются на территории Казахстана, стран СНГ и дальнего зарубежья;
- имеют международную регистрацию ISSN (Париж);
- публикуют статьи на 3-х языках: казахском, русском и английском в рамках рубрик: «Экономика», «Философия», «История», «Социология», «Политика» и «Культурология»;
- осуществляют подписку через
АО «Казпочта»,
ТОО Агентство «Евразия-Пресс»,
ТОО «KazPress»,
ТОО «Эврика-Пресс»

Подписной индекс журнала
«САЯСАТ-POLICY» – 75861,
цена подписки на 2013 год – 7200.0 тенге

Подписной индекс журнала
«ЕВРАЗИЙСКОЕ СООБЩЕСТВО» – 75760,
цена подписки на 2013 год – 4000.0 тенге

Кроме статей, публикуем материалы
конгрессов, конференций и
других мероприятий,
а также размещаем рекламу

По вопросам размещения статей,
рекламы и Ваших пожеланий

УСЛОВИЯ РАЗМЕЩЕНИЯ ПУБЛИКАЦИЙ В ЖУРНАЛЕ:

Статья должна сопровождаться:
- рекомендацией (отзывом) учреждения, в котором выполнена работа, заверенная печатью;
- разрешением на публикацию в открытой печати (экспертное заключение), заверенное печатью.

Реферат статьи (резюме), представленный на 3-х языках (каз., рус., англ.) на отдельной странице после статьи, должен содержать не более 2-3 предложений и не повторять название статьи.

Статья предоставляется на CD-носителе (с обязательной распечаткой текста в редакторе Microsoft Word, шрифтом TimesNewRoman 10, через 1,5 интервала, в 1-м экз.; поля: верхнее и нижнее – 20 мм, левое – 30 мм, правое – 15 мм, объемом 4-6 страниц).

Иллюстрации к статье предоставляются в исходном формате (т. е. диаграмма в Excel, карты в COREL DRAW и т.д.).

Статья подписывается автором (авторами) в нижнем правом углу на каждой странице текста.

Ссылки на литературу в тексте обозначаются арабскими цифрами в квадратных скобках. Список литературы помещается после статьи (описание каждого источника включает: фамилию и инициалы автора, название работы (при необходимости сборника, журнала и т.п.), место издания (город и из-
[illegible] и коли-
[illegible]ается над
таблицей со с[illegible]

Название р[illegible]
рисунком с пр[illegible]
на этот рисунок.

На отдельной странице сле[illegible]
вести Ф.И.О полностью, до[illegible]
ученую степень (если таковая имеется), город, место работы, служебный и домашний телефоны, e -mail.

Сокращенные и условные обозначения допускаются лишь принятые в международной системе единиц сокращения мер, физических, химических и математических величин, терминов и т.п.

Статья в журнал «Саясат-Policy» может быть представлена на одном из

КОМПЬЮТЕРНЫЙ ТЕРРОРИЗМ: СУЩНОСТЬ, СОВРЕМЕННОЕ СОСТОЯНИЕ И ПРОГНОЗЫ РАЗВИТИЯ

Калиев И.А. – к. п. н., доцент
(г. Павлодар, ПГУ им. С. Торайгырова)

Масштабные террористические действия, имевшие место в последние годы в различных регионах мира, и сопряженные с этим невосполнимые человеческие жертвы заставляют по-новому взглянуть на проблему терроризма, которая сегодня превратилась в реальную и серьезную угрозу стабильности и безопасности социального мира и прогресса человечества.

Особенности развития процессов глобализации в современных условиях обусловлены переходом от общества индустриального к информационному. Внедрение новейших технологий во все сферы жизнедеятельности общества формирует иные потенциалы для стран с транзитивной экономикой. Это касается, и политики, и самого государства, а также всего общества и сознания его граждан.

Практически каждая отрасль в хозяйстве страны, включая энергетику, транспорт, связь, банковский сектор и т.д., использует компьютерные сети и, соответственно, зависит от их работоспособности. Нарушив работу этих сетей, можно парализовать инфраструктуру страны. Таким образом, быстрый прогресс в развитии информационных технологий приводит к возникновению новых существенных проблем в сфере международной безопасности и стабильности и может иметь неожиданные последствия в виде растущей уязвимости систем.

По мнению ряда международных экспертов, проблемы безопасности занимают среди проблем дальнейшего развития киберпространства одно из центральных мест, а вопрос о контроле информационного пространства становится все более актуальным и должен рассматриваться и решаться немедленно [1].

В этом контексте, одной из новых и опасных угроз человечеству становится использование террористическими организациями новейших информационных технологий. Согласно исследованиям ряда отечественных ученых и данных зарубежных исследовательских центров, терроризм стал международной индустрией, способной распоряжаться огромными информационными, финансовыми, технологическими и другими возможностями [2].

Поэтому исследование феномена компьютерного терроризма (кибертерроризма) в контексте информационной политики становится важным аспектом национальной и международной безопасности.

Сама природа компьютерных преступлений и компьютерного терроризма является всемирной проблемой, поскольку не имеет значения, где именно совершено подобное преступление. Поэтому рассмотрим, что такое компьютерный терроризм более детально.

Под «компьютерным терроризмом» следует понимать сознательное, целенаправленное применение компьютерной информации, компьютеров, компьютерных систем и сетей для захвата компьютерных систем управления потенциально опасными объектами с целью:

а) вывода этих объектов из строя или их разрушения, что прямо или косвенно создает или угрожает возникновением чрезвычайной ситуации вследствие этих действий и представляет опасность для персонала, населения и окружающей среды;

б) создания условий для аварий и катастроф техногенного характера;

в) запугивания населения и органов власти угрозами совершения вышеуказанных противоправных действий;

г) совершения провокаций военного конфликта и возникновения международных осложнений;

д) оказания влияния на принятие решений, совершения или несовершения действий органами государственной власти или органами местного самоуправления, должностными лицами этих органов, объединениями граждан, юридическими лицами, обеспечения организационного или иного содействия созданию или деятельности террористической группы или террористической организации [3].

Таким образом «компьютерный терроризм» проявляется в двух аспектах – технологическом и информационном. Технологический аспект компьютерного терроризма связан с технологической формой проявления различных видов терроризма – использованием компьютерных технологий для совершения террористических действий.

Информационный аспект связан с осуществлением с помощью компьютерной информации воздействия на психику и сознание людей, с целью формирования нужных мыслей и суждений, определенным образом направляющих поведение людей в нужном для террористов направлении. При этом компьютеры, компьютерные системы и сети выполняют роль средства доставки такой информации до потребителей – пользователей глобальных сетей [4].

Что касается технологического аспекта компьютерного терроризма, то в подавляющем большин-

стве ранних работ, посвященных компьютерному терроризму, преувеличиваются возможности кибертеррористов. Так, экспертом по вопросам терроризма, директором Международного центра исследования терроризма при Потомакском институте политических исследований в Вашингтоне профессором Иона Александером (Yonah Alexsander), было высказано следующее предостережение: «Следует ожидать эскалации террора во всем мире ... Будет практиковаться также кибертерроризм – преступники попытаются одним нажатием клавиши нарушить, например, энергоснабжение целого района или работу аэропорта» [5].

Но это не подкрепляется никакими фактами. Брюс Шнайер, основатель компании Counterpane Internet Security и известный специалист по криптографии, вообще считает, что угроза кибертерроризма, о которой говорят многие правительственных органов и спецслужбы, сегодня переоценивается [6].

Более тщательное изучение взаимосвязи компьютерных сетей и важнейших инфраструктур, их уязвимости к атакам и значения нападений для национальной безопасности, дает основания считать, что имеющиеся данные об уязвимости недостаточно верны. Поэтому, для исследования уязвимости важнейших инфраструктур к проявлениям компьютерного терроризма необходима гораздо более детальная оценка каждой из них, а именно: оценка избыточности инфраструктуры, норм сбоев, степени человеческого участия в процессах управления и контроле, вмешательство человека в критических ситуациях.

Вообще переоценка угрозы компьютерного терроризма в технологическом аспекте базируется на анализе кибератак на фоне происходящих обычных аварий, в частности: отключении электроэнергии, задержки полетов, аварий на коммуникациях и их последствия, что является индикатором для определения возможных последствий компьютерного терроризма также – определения степени зависимости ключевых инфраструктур от компьютерных сетей.

Анализ последних научных работ и публикаций в СМИ о деятельности террористических организаций в информационном пространстве показал, что наибольший интерес для террористов составляют: энергетическая сфера, военная и ядерная структура государства, сфера транспортных перевозок (особенно воздушный транспорт) и финансовая сферы государства. При этом, проанализировав каждую из этих структур, можно утверждать, что они не так уязвимы к киберугрозам, как это освещается в СМИ.

Исследования, проведенные Информационной группой Комиссии по консультациям в области безопасности национальных телекоммуникаций США по уязвимости систем электроснабжения кибератакам, показали, что «физическое разрушение все еще представляет наибольшую угрозу, с которой может столкнуться энергетическая инфраструктура. Наряду с этим уже появилась проблема электронного вторжения, но она все еще составляет относительно небольшую опасность» [7].

Что касается другой угрозы, довольно часто упоминается СМИ в контексте компьютерного терроризма, – угроза военным структурам государства. Однако, несмотря на регулярные сообщения СМИ о десятках тысяч ежегодных нападений на сети различных военных объектов, ни в одной стране не наблюдалось деградации военных возможностей.

Еще одна тема, которая постоянно обсуждается, – вмешательство в национальные системы транспортных перевозок, с целью выведения их из строя. Но, говоря о системе управления транспортным движением, эксперты по кибербезопасности отмечают ее выделенность из системы, связанной с сетью Интернет, поэтому захватить самолет или поезд «дистанционно» в принципе невозможно [8].

По мнению экспертов, из всех перечисленных сфер жизнедеятельности человека наиболее открытой для глобального информационного пространства является именно финансовая сфера, которая является привлекательной для потенциальных киберугроз – вмешательство в работу банков, фондовых бирж, срыв международных финансовых сделок. Это связано с тем, что сегодня вся финансовая система ориентирована на упрощения доступа клиентов к банковским, торговым и биржевым услугам с использованием новых информационных технологий (в том числе и осуществления многих операций в сети Интернет) [9]. В этом контексте целесообразно привести данные из публикаций китайских военных журналов, где некоторые авторы высказывали мнение о возможности с помощью кибератак вывести из строя американские финансовые рынки. Но Китай настолько же зависит от этих финансовых рынков, насколько и США и от сбоя может пострадать даже больше [10].

Таким образом, следует сделать вывод, что в контексте макроэкономики сбои в системах электроснабжения, сбои в функционировании транспортного движения и другие «сценарии» кибертеррора – стандартные события, которые не касаются национальной безопасности. Для национальной экономики, где десятки или даже сотни систем обеспечивают важнейшие инфраструктуры, сбой в системах вследствие кибератаки может остаться незамеченным в повседневной жизни или быть отнесенным к стандартным задержкам и выходу из строя оборудования (кроме случаев, когда атака будет совмещена с физическим нападением – применением огнестрельного оружия, взрывами, захватом стратегически значимых объектов).

Кибератаки не могут иметь такого драматического и политического эффекта, к которому стремятся террористы. С целью запугивания и достиже-

ния своих стратегических целей, или любого значимого эффекта кибертеррористы должны атаковать множество целей одновременно и продолжать атаки в течение достаточно длительного периода.

Для большинства важнейших инфраструктур такой сценарий многочисленных нападений невозможен для хакеров, террористических групп или государств. Так, согласно докладу CNet. com report, аналитики информационной безопасности пришли к выводу, что для достижения успеха подобной атаки террористам «потребуется организация, которая имеет значительные ресурсы (примерно 200 млн. дол. США), мощную разведку и пять лет для подготовки» [11].

По мнению отдельных специалистов, сегодня не существует убедительных доказательств того, что любая террористическая организация готова использовать компьютеры для серьезной разрушительной деятельности. Военные аналитики-эксперты корпорации RAND Сет Джонс (Seth G. Jones) и Мартин Либицки (Martin C. Libicki) считают, что «нет никаких доказательств того, что люди, известные нам как террористы, собираются заниматься кибертерроризмом и планируют использовать Интернет не только для коммуникации и координации атак традиционного типа, но и для кибератак» [12].

В докладе Главного контрольного управления Сенатского комитета по государственным делам США относительно угроз критически важным элементам инфраструктуры отмечалось, что «до сих пор ни одна из традиционных террористических групп, такая, как Аль-Каида», не использовала Интернет для атак на инфраструктуры государств [13]. Ричард Кларк (Richard A.Clarke), бывший координатор Белого дома по вопросам терроризма, охотно признает, что «до этого времени вообще не видел известных террористических групп, осуществляющих кибератаки против государств» [14].

Профессор права Университета штата Огайо Петер Свайр (Peter Swire) отметил, что «сегодня распространение мнения о неотвратимости угрозы компьютерного терроризма, прежде всего полезно крупным ИТ-компаниям, которым из-за перенасыщения рынка технологиями необходимо найти новые источники дохода. Одним из таких источников является государственное финансирование проектов, связанных с новыми затратами на ИТ-безопасность» [15]. Учитывая это, проблема кибербезопасности в контексте терроризма представляется сомнительной.

Такого же мнения придерживается профессор Джорджтаунского университета Дороти Деннинг (Dorothy E. Denning), одна из самых авторитетных экспертов в области компьютерной преступности и кибербезопасности, которая отмечает, что кибертерроризм нельзя сравнивать с химическим, биологическим или ядерным оружием, его даже нельзя считать такой же серьезной угрозой, как заминированные автомобили или террористы-самоубийцы [16].

Между тем многие специалисты склоняются к мнению, что атаки на компьютерные сети извне ограничивались модификациями официальных сайтов и не могли иметь непредсказуемые последствия. «Сломать сайт не трудно, трудно сделать так, чтобы это привело к действительно серьезным последствиям, – считает Мартин Либицки, – нанести серьезный ущерб, даже террористу, который знает компьютерные технологии, гораздо сложнее, чем считается» [17].

Кроме того, при анализе угрозы компьютерного терроризма обращает на себя внимание тот факт, что большинство инцидентов компьютерного проникновения на потенциально опасные объекты, связанные с терроризмом в киберпространстве, на самом деле не имеют политической окраски, это лишь проявления активности обычных компьютерных преступников, целью которых является получение материальной выгоды, удовлетворения исследовательского интереса или месть. Так, инциденты, которые произошли за последние годы, свидетельствуют, что сегодня их совершают скучающие подростки или инсайдеры.

Учитывая вышеизложенное, необходимо отметить, что при значительной уязвимости компьютерных сетей, которая существует сегодня, важнейшие инфраструктуры государства достаточно защищены.

Относительно информационного аспекта компьютерного терроризма следует отметить, что в данном случае отрицать его разрушительный характер было бы неверно. В контексте информационной безопасности все большую опасность представляет всемирная глобальная сеть Интернет, которая из-за своей открытости и анонимности становится главным «информационным полем», которое используют террористические организации в своих целях:

- сбор средств для поддержки террористической деятельности (в том числе путем мошенничества, вымогательства и шантажа);
- распространение агитационно-пропагандистской информации о деятельности террористических организаций, их целях и задачах, намерениях, формах протеста, обращения к массовой аудитории с сообщениями о признании своей ответственности за совершенные теракты и т.п.;
- осуществление организационной деятельности, например, размещение в открытом доступе и рассылка открытых и зашифрованных инструкций (например, инструкций по самостоятельному изготовлению взрывных устройств), сообщений о встречах заинтересованных лиц и т.д.;
- анонимное привлечение к террористической деятельности соучастников, например, хакеров и представителей бизнеса, которые предоставляют различные информационные услуги на коммерческой основе;

- планирование и координация действий, которая дает возможность децентрализовать управление террористическими организациями и расширить потенциал малых террористических групп;

- осуществление информационно-психологического воздействия на население с целью шантажа, создания паники и распространения дезинформации и т.д.

Кроме того, на данном этапе террористы сосредоточивают свои усилия на сборе информации и формировании баз данных. В этом контексте террористы преследуют две основные цели. Одна – формирование компромата (на основании полученных персональных данных о частной жизни руководителей стран, банков и корпораций), благодаря которому можно попытаться повлиять на руководителей разных уровней и получить доступ к необходимым информационным ресурсам страны или корпорации.

Другая – создание баз разведывательных данных, которые используются при подготовке атак. Например, японская террористическая группировка «Аум Синрике», которая осуществила газовую атаку в токийском метро в 1995 году, перед этим создала компьютерную систему, которая была способна перехватывать сообщения полицейских радиостанций и отслеживать маршруты движения полицейских автомобилей [18].

Вместе с тем, по мнению Даниэла Ларкина (Daniel Larkina), руководителя Центра регистрации Интернет-преступлений ФБР, оценка потенциальной опасности и ущерба, который может быть нанесен террористами, завладевшими персональными данными, является завышенной в разы. Эта информация не всегда используется, а потому интерес вокруг этой проблемы является чрезмерным. Чаще фиксируются не факты хищений информации, а попытки ее использования в коммерческих целях [19].

По мнению современных специалистов по компьютерному терроризму, сегодня основной целью террористов, прежде всего, является осуществление массового деструкционного воздействия на психику и сознание, людей в нужном для них направлении, с использованием информационных систем и систем связи. Можно предположить, что главным направлением кибертеррористов в будущем будет создание систем дистанционного манипулирования сознанием как конкретного человека, так и общества в целом [20]. Поэтому такое использование террористическими организациями информационных технологий и глобальной сети Интернет в недалеком будущем может стать одной из новых и опасных угроз человечеству.

Подытоживая изложенное, можно прогнозировать развитие компьютерного терроризма в дальнейшем и предоставить некоторые предложения по эффективному противодействию этому явлению.

Так, анализ характеристик и проявлений компьютерного терроризма позволяет сделать вывод, что террористическая активность различного рода экстремистских организаций в ближайшее время сохранится, как минимум, на прежнем уровне. При этом, масштабы и география террористических акций, с целью усиления деструктивного влияния на состояние политической, экономической и экологической безопасности государств мирового сообщества, возможно будут расширяться.

Терроризм разрабатывает множество новых стратегий для достижения своих целей. Среди них есть и такие, которые ориентированы не столько на проведение традиционных командных операций по уничтожению конкретных целей, сколько на дезинтеграцию тех или иных систем с помощью «информационных операций», а также координированных атак. При этом, некоторые специалисты считают, что именно «информационный потенциал» (коммуникационные каналы и контент-сообщения) может стать ключевой целью террористов.

В частности, некоторые специалисты по кибербезопасности прогнозируют, что «новые террористы» направят свои усилия на освоение информационного оружия, разрушительная сила которого может быть во много раз больше биологического и химического [21]. Приведенное позволяет сделать вывод, что терроризм эволюционирует в направлении, которое называют «информационной (сетевой) войной».

Именно поэтому противодействие проявлениям компьютерного терроризма требует комплексного подхода, объединяющего силовые, политико-дипломатические, экономические и гуманитарные формы и методы действий, а также эффективного сочетания антитеррористических мер, принимаемых на национальном и международном уровнях.

В противостоянии с новой террористической угрозой можно выделить ряд основных направлений борьбы:

- унификация и гармонизация национальных законодательств и международных актов, суть которых должна быть направлена на предупреждение и предотвращение компьютерного терроризма;

- разработка единого понятийного аппарата;

- совершенствование критериальной основы безопасности информационных систем;

- создание специализированных подразделений в сфере борьбы с компьютерными преступлениями и компьютерным терроризмом с эффективной системой координации их взаимодействия;

- совершенствование международного организационно-правового взаимодействия по вопросам противодействия компьютерной преступности и компьютерному терроризму;

- совершенствование многоуровневой системы подготовки кадров в сфере информационной безопасности.

Столь масштабная задача требует много времени и существенных финансовых затрат. Однако, современная реальность такова, что существование той или иной страны во многом определяется ее способностью своевременно формировать эффективный ответ на вызовы внешнего мира. Поэтому вопрос о функционировании эффективной национальной системы противодействия компьютерному терроризму – это вопрос о выживании развитых государств в современных условиях.

ЛИТЕРАТУРА

1. Dertouzous Michel L. What will be: How the New World of Information will Change our Lives. – Piaktus, 1997. – 384 p., Webster Frank. Theories of the Information Society. – London: Routledge, 2006. – 320 p.

2. Власихин В.А. «Патриотический акт»: юридический анализ. [Электронный ресурс]. – Режим доступа: <http://www. agentura. ru/ dossier/usa/ zakon-antiterror/>., Терроризм как угроза национальной безопасности. – 2004. [Электронный ресурс]. – Режим доступа: <http://www. regions. ru>.

3. CRS report 32114. Computer attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress. October 17, 2003. – pp. 4-5.

4. Тимати Л. Томас. Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху// Мировое сообщество против глобализации преступности и терроризма. Материалы международной конференции. – М., 2002. – С. 164–175.

5. Yonah Alexsander. Combating Terrorism: Strategies of Ten Countries // University of Michigan Press (August 7, 2002). – 448 p

6. Шнайер Брюс. Угроза кибертерроризма переоценена, 24 ноября 2005 года. [Электронный ресурс]. – Режим доступа: <http://www. ibusiness. ru/ news/ 240221/page2. html>.

7. Strategic Goal One: Keep America Safe by Enforcing Federal Criminal Laws (Fiscal Year 2000 Performance Report and Fiscal Year 2002 Performance Plan). – P. 25. [Електронний ресурс]. – Режим доступа: <http://www. usdoj. gov/ag/ annualreports/pr2000/ NewSG1. pdf>

8. Лукацкий А. «Безопасность сетей: Кибертерроризм: За и Против» [Электронный ресурс] // КомпьютерПресс. – 2001. – № 11. – Режим доступа к журналу: <http://www. compress. ru/article. aspx? id=12296&iid=465>

9. Гриняев С.Н. Информационный терроризм: предпосылки и возможные последствия. [Электронный ресурс]. – Евразийский вестник. – № 19, Режим доступа к журналу: <www. e-journal. ru/ besop-st3-19. html>.

10. James A. Lewis Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats // Center for Strategic and International Studies, Washington, D. C., December, 2002. [Электронный ресурс]. – Режим доступа: <www. csis. org/media/csis/pubs/021101_ risks_of_cyberterror. pdf>.

11. Joshua Green. The Myth of Cyberterrorism: There are many ways terrorists can kill you computers aren't one of them. – Washington Monthly, November, 2002. [Электронный ресурс]. – Режим доступа: <http://www. washingtonmonthly. com features/2001/0211. green. html>

12. Seth G. Jones, Martin C. Libicki. How Terrorist Groups End Implications for Countering al Qa'ida, 2008. [Электронный ресурс]. – Режим доступа: <http://www. rand. org/pubs/research_briefs/RB9351>.

13. Government Accountability Office U. S. [Электронный ресурс]. – Режим доступа: < http://www. gao. gov>.

14. Richard A. Clarke. Against All Enemies: Inside America's War on Terror // Free Press; 1St Edition edition (March 22, 2004). – 304 p.

15. The Security Traders. By Brendan I. Koerner | Sun September 1, 2002 12:00 AM PST. [Электронный ресурс]. – Режим доступа: <http://www. motherjones. com/print/15774>

16. Denning D.E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. [Электронный ресурс]. – Режим доступа: <http://www. nautilus. org/archives/info-policy/ workshop/papers/denning. html>

17. Seth G. Jones, Martin C. Libicki. How Terrorist Groups End Implications for Countering al Qa'ida, 2008. [Электронный ресурс]. – Режим доступа: <http://www. rand. org/pubs/research_briefs/RB9351>

18. Verton D. Black Ice: The Invisible Threat of Cyberterrorism. – N. Y, 2004. – 304 p.

19. Роговский Е.А. Россия в борьбе с международным терроризмом. Грани повышения позитивного образа страны. [Электронный ресурс] // Россия и Америка в XXI веке. – 2007. – № 3. – Режим доступа к журналу: <http://www. rusus. ru/? act=read&id=66>

20. Клепов А. Кибертерроризм и свобода личности. [Электронный ресурс]. – Режим доступа: <http://www. proza. ru/2009/04/10/500>

21. Walter Laqueur, «Postmodern Terrorism» Foreign Affairs, Vol. 75, № 5, September / October 1996. – pp. 24-36., John Arquilla, David Ronfeldt, and Michele Zanini. «Networks, Netwar, and Information-age Terrorism» in Michael Jenkins eds. «Countering the New Terrorizm». RAND Air Force federally funded research and development center (FFRDC) 1998. – pp. 39-82.