УДК 323.285

Современное состояние проблемы сетевой безопасности в Китае: кибертерроризм и механизмы борьбы с ним

Чжан До
Аспирант,
Дальневосточный федеральный университет (филиал в г. Уссурийске),
692519, Российская Федерация, Уссурийск, ул. Октябрьская, 71;
e-mail: zhangduo@yandex.ru

Аннотация

В статье рассмотрен новый вид террористической деятельности – кибертерроризм как глобальная надгосударственная проблема. Автором дается анализ деятельности террористических организаций в интернет-пространстве, описаны способы применения интернета в качестве средства распространения информации, пропаганды террористических действий, сбора сведений и средств, вербовки и т. д. Отмечается влияние кибертерроризма на различные сферы деятельности общества и социальные процессы. Цель работы заключается в определении понятия «кибертерроризм» и принципов борьбы с ним. Исследуются как подходы к пониманию самого понятия, так и способы противодействия ему мирового сообщества. В статье охарактеризована деятельность международных организаций и отдельно Китая в рамках борьбы с терроризмом, поднята проблема отсутствия единого понимания и единых путей решения существующей проблемы со стороны руководителей разных стран. Также автор выносит рекомендации по содействию антитеррористической борьбе в области сетевой безопасности, определяя главным направлением совместных усилий единый подход, а также всесторонний охват данного вопроса.

Для цитирования в научных исследованиях

Чжан До. Современное состояние проблемы сетевой безопасности в Китае: кибертерроризм и механизмы борьбы с ним // Теории и проблемы политических исследований. 2017. Том 6. № 3А. С. 330-342.

Ключевые слова

Кибертерроризм, сетевой терроризм, глобальная Сеть, киберпреступность, сетевая безопасность.

Введение

Интернет является не только важным связующим звеном между различными мировыми культурами, но и важным инструментом для обмена политической, экономической, торговой, потребительской и т. д. информацией. Совершенствование интернет-технологий дает новые стимулы для развития всех стран, а «жители» глобальной Сети приобрели неограниченные возможности в распространении идей массовому респонденту.

По мере роста объема интернета в жизни человека продолжает расти и число его активных пользователей, чем пользуются различные преступные элементы, в том числе и запрещенные террористические организации. Они используют интернет для расширения своего влияния, распространения насильственной информации, подстрекательских заявлений и действий. Преступники постоянно воздействуют на общественное сознание, умело используя его в своей террористической деятельности [Вейманн, 2004, 3]. Сетевой терроризм стал важным средством пропаганды. Так, например, «Восточный Туркестан» согласно статистическим данным за 2010-2014 годы выложил в Сеть 282 аудио- и видеоматериала, и их количество растет год за годом [Гу, 2014]. Исследователь Международного института по борьбе с терроризмом (Израиль) Майкл Барак на Всемирной интернет-конференции 2014 года отметил, что некоторые международные террористические организации используют сетевые технологии для вербовки и подготовки новых террористов, сбора средств и разведывательных данных, для запуска серии террористических атак [Барак, 2014].

Международное сообщество в борьбе с кибертерроризмом

Международное сообщество решительно отреагировало на действия кибертеррористов. Организация Объединенных Наций, включая Генеральную Ассамблею и Совет Безопасности, приняла резолюции, призывающие международное сообщество сотрудничать в борьбе с терроризмом. В Глобальной контртеррористической стратегии Организации Объединенных Наций, рассмотренной и принятой на 68-й сессии Генеральной Ассамблеи ООН в июле 2014 года, на основе поправок, сделанных Китаем, тема киберпреступности впервые была включена в текст документа [Ли, 2014]. Однако в 13 международной конвенции о борьбе с терроризмом в рамках ООН до сих пор нет специальной договоренности по вопросам кибертерроризма. Кроме того, перед международным сообществом стоят серьезные проблемы в данной области, одной из которых является отсутствие консенсуса в определении «кибертерроризма», что весьма затрудняет разработку международных конвенций по борьбе с этим явлением. Однако в данном документе с основой на понятие «киберпреступность» проанализировано действующее законодательство международной конвенции о контратаках на действия кибертеррористов, а также действующие законодательные положения о борьбе с киберпреступностью в Китае.

Что касается определения киберпреступности, то международное сообщество еще не сформировало единого понимания. Барри К. Коллин, старший научный сотрудник Калифорнийского института безопасности и разведки, в 1996 году впервые ввел термин «кибертерроризм». С тех пор ученые стали анализировать его как явление. Большинство людей считают, что киберпреступность – явление надгосударственное, целью и результатом такой деятельности является организация и реализации насильственных инцидентов. Представитель Федерального бюро расследований США Марк Поллитт утверждает, что кибертеррористы являются «субнациональными группами или подпольными агентами». Компьютерные системы, программы и данные помогают совершать преднамеренные, политически мотивированные атаки, которые приводят к насильственным действиям» [Чжоу, 2012]. Кроме того, в Соединенных Штатах широко известны криптографы, киберпреступники. Профессор Габриэль Вейманн, известный исследователь в области кибертерроризма из Хайфского университета в Израиле, определяет кибертерроризм как «использование компьютерных сетевых инструментов для уничтожения или закрытия национальной инфраструктуры (например, энергетики, транспорта, государственных операций и т. д.)» [Вейманн, 2004; Куин, 2013; Фу, 2014].

В ответ на использование интернета для террористической деятельности Целевая группа по осуществлению контртерроризма (CTITF) представила отчет (2009) с перечнем способов и целей использования кибертеррористами Интернета: 1) для совершения террористических атак посредством дистанционного изменения информации в компьютерной системе или вмешательства в обмен данными между компьютерными системами; 2) как информационного ресурса; 3) в качестве средства пропаганды и массового распространения идей; 4) в целях поддержки и осуществления террористической деятельности. Существует множество форм кибертеррористической деятельности, в том числе «кибератаки, использование интернета для привлечения капитала, вербовка и обучение террористов с помощью интернета, обучение, сбор данных, подстрекательство к террористическим заявлениям и т. д.» [Сун, 2013].

Определение кибертерроризма в докладе CTITF гласит: «Терроризм является основным способом насилия, а цель террористических организаций – публично передавать насилие посредством Сети для достижения политических и социальных целей» [Организация Объединенных Наций в борьбе с терроризмом, www]. Доклад CTITF Организации Объединенных Наций содержит более полное изложение элементов киберпреступности, а именно намерений, целей и результатов кампаний, а также террористических актов, которые выступают и как средство, и как объект нападения.

Сетевой терроризм (киберпреступность в целом) как международное явление стал основной проблемой международного сообщества. Поэтому странам необходимо выработать курс на укрепление международного консенсуса и создание единых стандартов в определении кибертерроризма. В целях укрепления международного сотрудничества в борьбе

с кибертеррористическими актами, привлечения к ответственности и наказание виновных в кибертеррористической деятельности, разработки международных конвенций против киберпреступности государствам в рамках работы Организации Объединенных Наций необходимо учитывать новые условия развития международного сообщества.

С 1990-х годов официально был выдвинут термин «кибертерроризм». В XXI веке информационного общества кибертерроризм и информационная война стали новой формой терроризма [Yonah, Carlton, Wilkinson, 1979 , 59]. Однако мировым сообществом использование интернета для террористических целей отмечалось давно. Как указано в плане действий Глобальной контртеррористической стратегии ООН, принятой в 2006 году, «Организация Объединенных Наций изучает пути и средства использование интернета в качестве инструмента борьбы с распространением терроризма, соблюдая права человека и другие обязательства по международному праву с должным учетом конфиденциальности, признавая при этом, что некоторым государствам, возможно, потребуется сделать это в контексте необходимости борьбы с распространением терроризма на международном и региональном уровнях и в борьбе со всеми формами и проявлениями терроризма в Интернете» [Глобальная контртеррористическая стратегия…, 2006]. Последующие «Контртеррористическая стратегия ООН на 2008 год», «Контртеррористическая стратегия ООН на 2010 год» и «Контртеррористическая стратегия ООН – 2012» также были введены с целью борьбы с кибертерроризмом.

Совет Безопасности Организации Объединенных Наций принял также соответствующие резолюции, в которых содержится призыв к государствам-членам бороться с кибертеррористической деятельностью: резолюции Совета 1963 года № 2129, принятые Советом [Организация Объединенных Наций в борьбе с терроризмом, www; Официальные документы Совета Безопасности…, 2014, www]. В резолюциях Организации Объединенных Наций по глобальной контртеррористической стратегии и Совета на 2006-2006 годы предусматриваются общие требования к борьбе с киберпреступностью, однако не представлено конкретных ответов, а также каких-либо указаний относительно наказания виновных в совершении преступлений. Следовательно, современное международное сообщество по борьбе с кибертеррористической деятельностью может опираться только на существующие положения конвенций Организации Объединенных Наций по борьбе с терроризмом.

Опыт Китайской Народной Республики в борьбе с кибертерроризмом

В целях борьбы с кибертерроризмом правительство Китая предпринимает множество средств. Во-первых, согласно закону о борьбе с кибертерроризмом, уголовное законодательство Китая обеспечивает процессуальные гарантии соблюдения критериев и оснований для вынесения приговора. Судебная система Китая действует в соответствии с законом в целях борьбы с хранением, производством и распространением преступниками террористическо-

го аудио и видео. Во-вторых, существует сеть интернет-предприятий, специализирующихся на исследовании Сети в террористической зоне. Интернет-операторы Китая, поставщики услуг, сознательно отвечающие за антитеррористические обязательства, под руководством правительства берут на себя инициативу по очистке информации в интернете. В-третьих, имеет место широкое вовлечение граждан и общественных организаций в антитеррористическую деятельность, их поощрение китайским правительством за активное участие в борьбе с кибертерроризмом. Некоторые интернет-компании создают на своих сайтах платформу для размещения гражданами и общественными организациями сообщений о незаконной онлайн-информации. Также активно поддерживаются международные организации. Ввиду того, что террористические организации «Восточного Туркестана» используют зарубежный интернет для распространения своей информации, определенные ведомства китайского правительства активно общаются с соответствующими странами, организациями и предприятиями и добились определенных результатов в совместной работе.

Двенадцатая сессия Постоянного комитета двенадцатого Всекитайского собрания народных представителей приняла 1 июля 2015 года «Закон о национальной безопасности Китайской Народной Республики». Проект Закона КНР «О безопасности в Интернете» 6 июля был опубликован, что стало важным шагом в деле сохранения безопасности страны. В декабре того же года на 18-м заседании двенадцатого Всекитайского собрания народных представителей принят «Закон о борьбе с терроризмом», который стал первым специальным антитеррористическим законом Китая [Ин Чэнь Лин, 2015].

Для адаптации «Закона о борьбе с терроризмом» к нынешним усилиям борьбы Китая с террористическим насилием необходимо было обеспечить прочную правовую основу. С этой целью китайское правительство провело обширные исследования зарубежного опыта (в частности, законодательный опыт США, стран-членов Европейского Союза, таких как Германия, Великобритания, Нидерланды [Контртерроризм в Китае необходим, 2015, www; Цзян, 2016]), рассмотрело различные мнения о фактической ситуации и неотложных потребностях внутренней антитеррористической работы, особенно в плане определения обязательств сетевых операторов и поставщиков сетевых услуг.В положениях статей 18 и 19 третьей главы «Закона о борьбе с терроризмом» проблема безопасности рассматривается в связи с деятельностью операторов телекоммуникационных компаний и поставщиков интернет-услуг. Статья 18 прямо предусматривает, что «операторы телекоммуникационных услуг и провайдеры интернет-услуг должны оказывать техническую поддержку и помощь органам общественной безопасности и органам национальной безопасности для предотвращения и расследования технического интерфейса и расшифровки террористической деятельности в соответствии с законом». Это положение согласуется с требованиями Совета Безопасности Организации Объединенных Наций.

В статье 19 предусматривается, что «операторы связи и провайдеры интернет-услуг в соответствии с положениями законов и административных регламентов осуществляют се-

тевую безопасность, систему надзора за информационным наполнением и предпринимают меры по осуществлению технологии безопасности для предотвращения распространения информации, содержащей террористический и экстремистский контент, в том числе информацию о терроризме, экстремистское содержание, передачу которого должны незамедлительно прекратить, сохранить соответствующие записи и удалить информацию, а также сообщить о ней органам общественной безопасности или соответствующим департаментам. Информация об экстремистском содержании должна быть выявлена вовремя в целях содействия расследованию. Трансграничная передача информации с террористическим и экстремистским содержанием запрещена, а органы электросвязи должны принимать технические меры для блокирования ее распространения» [Чжэн Чэн Си, 2010, 11]. Эта статья, как представляется, предусматривает меры, которые необходимо принимать в случаях кибертерроризма. Предпринимаемые Китаем усилия по выявлению, предупреждению и пресечению преступлений в интернет-сфере, во многом согласуются с положениями некоторых стран мира.

Положения «Закона о национальной безопасности», принятого в отношении безопасности киберпространства в июле 2015 года, носят более общий и принципиальный характер, требуя «укрепления сетевого управления, предотвращения, прекращения и наказания организаций, вторгающихся в Сеть, распространяющих незаконную информацию и совершающих иные преступные действия в целях защиты национальных интересов и киберпространства, интересов безопасности и развития» [Ин Чэнь Лин, 2015]. Исходя из этого, в Китае был рассмотрен, но еще не принят «Закон о сетевой безопасности». В нем в основном содержатся вопросы по операционной безопасности Сети, безопасности сетевых данных и правила сетевого сохранения информации.

Будучи одним из пяти постоянных членов ООН, Китай присоединился к подписанию 12 из 13 конвенций по борьбе с терроризмом, принятых в рамках Организации Объединенных Наций. Однако ни в одной из них не описано конкретных мер по противодействию кибертерроризму. Более того, понимание международным сообществом киберпреступности еще не унифицировано, и в этом вопросе не сформировано единого стандарта.

Система базы данных по борьбе с терроризмом в основном хранит и обрабатывает информацию, связанную с Сетью, и информацию, которая включает сведения о персонале, траектории передвижений людей или объектов. В базе хранятся записи о судимости, направлениях деятельности, перечень ответственных лиц, регистрации временного резидента, незаконный учет трафика, регистрационные записи пользователей, транзакции транспортных и денежных средств, запись о банковских операциях, регистрационные записи о проживании в гостинице и пр. Вышеуказанная информация временно хранится с использованием антитеррористической базы данных и автоматически создается по номеру ID-карты или номера паспорта. Эта система способствует привлечению внимания персонала, особенно для внедрения долгосрочных групп динамического мониторинга.

Система сбора информации также хранит и обрабатывает данные о всех видах террористических акций, происходящих внутри страны и за рубежом, имена членов террористических организаций, рабочие документы и т. д. Во-первых, обработка и анализ террористической информации департаментами по борьбе с терроризмом осуществляется на всех уровнях соответствующих подразделений в режиме реального времени. Аккумулируется текущая информация о новейших террористических действиях внутри страны и за рубежом для предотвращения террористических нападений. Во-вторых, в соответствующих департаментах происходит накопление и анализ информации о террористических организациях для своевременного выявления новых инцидентов. В-третьих, накопление антитеррористических сведений (включая антитеррористические законы, меры по предотвращению терроризма, данные разведки, антитеррористические исследования и т. д.) [Барак, 2014].

Отработан в Китае механизм заблаговременного предупреждения терроризма. Статья 47 «Закона о борьбе с терроризмом» предусматривает, что «Национальный информационный центр по борьбе с терроризмом, руководящие органы местной антитеррористической деятельности и органы общественной безопасности и другие соответствующие ведомства должны быть в доступе для разведывательной информации. Необходимо незамедлительно уведомить соответствующие департаменты и подразделения для возможности предупреждать об опасности в соответствии с ситуацией. Соответствующие департаменты и подразделения должны обеспечить безопасность сообразно полученным уведомлениям, а также в связи со сложившимися обстоятельствами обеспечить предотвращение и устранение проблемы» [Ли, 2014]. Для проверки или сбора соответствующих улик отдел по борьбе с терроризмом применяет подход «один случай – один отчет», который предоставляется в течение установленного периода и незамедлительно направляется в соответствующее подразделение и отделы для принятия решения в соответствии с выявленными уликами. Также создано антитеррористическое подразделение для предотвращения и предупреждения преступлений. То есть на всех уровнях функционирует система раннего предупреждения для эффективного осуществления плана предотвращения угрозы терроризма. Он включает в себя контроль, предупреждение и блокировку преступлений на разных этапах. В нем определены командиры, количество военных действий, перевозочное оборудование, средства безопасности, связь и превентивные меры [Фань, 2012].

Сетевая террористическая деятельность не ограничивается конкретной страной, регионом, поэтому какое-либо государство, организация или отдельный человек не могут быть защищена от нее. Нужно укреплять сотрудничество и совместные действия. С этой целью Китай выступает со следующими инициативами:

1) в первую очередь, упрочить мировой консенсус. Интернет-терроризм – болезнь всеобщая, наносящая вред международному сообществу. Все члены Организации Объединенных Наций идентифицировали террористические интернет-организации и все виды их деятельности в Сети как кибертеррористические акты. Все правительственные организации

должны взять на себя обязательства по борьбе с кибертерроризмом и быть ответственны за свои действия и предпринятые меры;

2) эффективно бороться с кибертерроризмом под эгидой правительств. Правительства в соответствии с требованиями резолюций Организации Объединенных Наций, международных конвенций и национальных законов активно координируют ресурсы и силы своих стран и берут на себя инициативу, сделая все возможное, чтобы и не предоставлять пространство для онлайн-деятельности террористических организаций;

3) добиться поддержки и активно вовлекать в борьбу с кибертерроризмом всех представителей общества. Каждая организация, предприятие и гражданин должны взять на себя инициативу. В частности, интернет-предприятия должны принять различные меры по пресечению каналов передачи информации и не дать террористам возможность использовать онлайн-пространство и технические средства;

4) укреплять сотрудничество. Интернет упрочивает международные связи, в том числе и в противостоянии киберпреступлениям. Необходимо упрочение сотрудничество, отработка механизмов коопреации между правительствами, организациями и предприятиями, налаживание обмена информацией между людьми. Совместная разработка прочной линии защиты от кибертерроризма обеспечит повышение благосостояния людей и стабильности во всем мире.

Заключение

Распространение терроризма стало очень важной глобальной проблемой и оказывает влияние на мировую экономику и политику, усугубляет противоречия международного сообщества, сказывается на стабильности и всем порядке глобального общества. Терроризм довольно сложный социальный феномен. Он основан на создании и усугублении противоречий существующей международной системой и включает в себя экономические, религиозные, политические, социальные и этнические разногласий.

Террористическая деятельность порождает недовольство, поэтому устранять терроризм довольно трудно и продолжительно о времени. Причины терроризма сложны, а его последствия имеют длительные перспективы. Различные позиции стран мира по проблеме терроризма будут вызывать международные политические разногласия и противоречия, что скажется на международной политической ситуации.

Библиография

1. Барак М. Многосекторальное сотрудничество против кибервойны (迈克尔·巴拉克：多部门合作打击网络圣战组织). 2014. URL: http: //media.people.com.cn/n/2014/1120/c120837-26061521

2. Вейманн Г. Как современный терроризм использует Интернет: специальный доклад № 116 // Владивостокский центр исследования организованной преступности. 2004.
3. Глобальная контртеррористическая стратегия Организации Объединенных Наций: резолюция Генеральной Ассамблеи ООН от 08.09.2006. URL: http://docs.cntd.ru/document/902114207
4. Гу Ч. Китайское правительство использует различные средства для борьбы с кибертерроризмом. URL: http://media.People.Com.Cn/n/2014/1120/c120837-26059821
5. Журнал Юньнаньского административного колледжа, 2012. № 3.
6. Жэньминь жибао. URL: http://inosmi.ru/people_com_cn/?id=236763177&date=20160604T051721
7. Ин Чэнь Лин. Рассмотрение законодательства по борьбе с терроризмом в целях улучшения сети // Информационная безопасность Китая. 2015. № 8. С. 43-45.
8. Йонах А. Терроризм в XXI веке: угрозы и ответы. 12 Depaul Bus. L.J. (1999/2000): 59. Yonah A., Carlton D., Wilkinson P. Terrorism: theory and practice. Boulder, Colo: Westview Press, 1979. 280 p.
9. Контртерроризм в Китае необходим. URL: http://www.Legaldaily.Com. /cn/commentary/content/2015-12/29/content_6423984.node=33188.Htm?Node=33188
10. Куин Б. Исследование преступлений седиментационного типа: защита конституционных прав. Пекин: Law Press, 2013.
11. Ли Б. Задачи и возможности для сетевых наук в исследовании антитерроризма // Комплексные системы и наука о сложностях. 2014. № 1(60).
12. Ли Х. Уголовное законодательство в «Поправке к Уголовному Кодексу (VIIII)», связанное с терроризмом, экстремизмом, преступностью // Журнал Цучжоуского университета. 2015. № 6.
13. Народная публичная информация о безопасности Китая. Пекин, 2005.
14. Организация Объединенных Наций в борьбе с терроризмом. URL: http://www.Un. Org/zh/terror/index.Shtml
15. Официальные документы Совета Безопасности Организации Объединенных Наций // Совет Безопасности Организации Объединенных Наций. 2014. URL: http://www.fr./documents/view_doc.asp?Symbol=S/RES/2133
16. Резолюция совместной работы государств-членов по предотвращению использования террористами технологий, средств связи и ресурсов для стимулирования поддержки террористических актов // Совет Безопасности Организации Объединенных Наций. URL: http://www.un.org/zh/sc/documents/resolutions/2010/s1963
17. Сун А. Международная антитеррористическая граница – терроризм. Международное право. Харбин: Хейлунцзянская образовательная пресса, 2013.
18. Сяофэн М., Сян Ц. Управление персональными данными: концепции, технологии и вызовы // Компьютерные исследования и разработки. 2013.

19. Фань Я. Использование сети для террористических преступлений – современная область борьбы с терроризмом – проблемы и трудности // Китайский журнал социальных наук. 2012. № A09, № A03, A08.
20. Фу Ц. Сетевое право – верховенство закона Китая в правильном смысле / Китайский журнал социальных наук. 2014. № A05.
21. Цзан Ц. Обзор уголовного законодательства по борьбе с терроризмом и «Закон о борьбе с терроризмом» Китая // Евразийский научный журнал. 2016. № 5.
22. Чжан М. В «Поправке к Уголовному Кодексу (VIIII)» о преступности терроризма // Современное право. 2016. № 1.
23. Чжоу Х. Понимание и применение нового террористического преступления в «Поправке к Уголовному Кодексу (VIIII)» // Китайский прокурор. 2015. № 10.
24. Чжоу Ц. Глобальное общество риска и информационное общество в уголовном праве:преобразование модели уголовного права в XXI веке. Пекин: Китайский издательский дом, 2012.
25. Чжэн Чэн Си. Обзор законодательства о безопасности информационной сети Китая // Новости интеллектуальной собственности Китая. 2010. № 1.
26. Чэнь. Необходимое главенство закона в борьбе с терроризмом в Китае (中国依法反恐势在必行). 2015. URL: http://www.Legaldaily.Com.Cn/commentary/content/2015-12/29/content_6423984.htm? node=33188

Current state of the problem of network security in China: cyberterrorism and means of fighting against it

Duo Zhang
Postgraduate,
Branch of Far Eastern Federal University in Ussuriysk,
692519, 71 Oktyabr'skaya st., Ussuriisk, Russian Federation;
e-mail: zhangduo@yandex.ru

Abstract

The article considers a new type of terroristic activity – cyberterrorism that has arisen recently and acquired the status of a global supranational problem immediately after its appearance. The author of this article analyses the terror organizations' activities of such kind and describes ways of using the Internet as a mean of spreading propaganda of terrorist actions. The author explores both points of view to understanding the concept of cyberterrorism and

ways of counteracting it in China and the world community. The influence of cyberterrorism on various spheres of social activity and the normal course of social processes is marked. The main objective of this article is the necessity to define the term of cyberterrorism and its influence on society. The author describes the activities of China and world organizations in the field of politics and legislation in the fight against terrorism, raises the problem of common misunderstanding and ways of influence of different countries on the problem. In addition, the author makes recommendations on the contribution to fight against network terrorism. A single standard and holistic view of the problem are defined as the mainstay of co-operative efforts. The author notices that the causes of terrorism are complex and it has long-lasting effect.

For citation

Zhang Duo (2017) Sovremennoe sostoyanie problemy setevoi bezopasnosti v Kitae: kiberterrorizm i mekhanizmy bor'by s nim [Current state of the problem of network security in China: cyberterrorism and means of fighting against it]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 6 (3A), pp. 330-342.

Keywords

Cyberterrorism, network terrorism, global network, cybercrime, network security.

References

1. Barak M. (2014) *Mnogosektoral'noe sotrudnichestvo protiv kibervoiny* [Multisectoral cooperation against cyber war]. Available at: http: //media.people.com.cn/n/2014/1120/c120837-26061521 [Accessed 15/06/17].
2. Chen' (2015) *Neobkhodimoe glavenstvo zakona v bor'be s terrorizmom v Kitae* [Necessary rule of law in combating terrorism in China]. Available at: http://www.Legaldaily.Com.Cn/commentary/content/2015-12/29/content_6423984.htm? node=33188 [Accessed 16/06/17].
3. Chzhan M.V. (2016) "Popravke k Ugolovnomu Kodeksu (VIIII)" o prestupnosti terrorizma [In the "Amendment to the Criminal Code (VIIII)" on the crime of terrorism]. *Sovremennoe pravo* [Modern law], 1.
4. Chzhen Chen Si (2010) Obzor zakonodatel'stva o bezopasnosti informatsionnoi seti Kitaya [Review of legislation on security information network of China]. *Novosti intellektual'noi sobstvennosti Kitaya* [News of intellectual property of China], 1.
5. Chzhou Kh. (2015) Ponimanie i primenenie novogo terroristicheskogo prestupleniya v "Popravke k Ugolovnomu Kodeksu (VIIII)" [Understanding and application of the new terrorist offences in the "Amendment to the Criminal Code (VIIII)"]. *Kitaiskii prokuror* [Chinese attorney], 10.

6. Chzhou Ts. (2012) *Global'noe obshchestvo riska i informatsionnoe obshchestvo v ugolovnom prave: preobrazovanie modeli ugolovnogo prava v XXI veke* [Global risk society and information society in criminal law: the transformation of criminal law in the XXI century]. Pekin: Kitaiskii izdatel'skii dom Publ.
7. Fan' Ya. (2012) Ispol'zovanie seti dlya terroristicheskikh prestuplenii – sovremennaya oblast' bor'by s terrorizmom – problemy i trudnosti [The use of the network for terrorist offences – a modern field of fight against terrorism – problems and challenges]. *Kitaiskii zhurnal sotsial'nykh nauk* [Chinese journal of social sciences], A09, A03, A08.
8. Fu Ts. (2014) Setevoe pravo – verkhovenstvo zakona Kitaya v pravil'nom smysle [Network law – the rule of law in China on proper meaning]. *Kitaiskii zhurnal sotsial'nykh nauk* [Chinese journal of social sciences], A05.
9. *Global'naya kontrterroristicheskaya strategiya Organizatsii Ob"edinennykh Natsii: rezolyutsiya General'noi Assamblei OON ot 08.09.2006* [Global counter-terrorism strategy of United Nations: Resolution of the UN General Assembly of September 08, 2006]. Available at: http://docs.cntd.ru/document/902114207 [Accessed 19/06/17].
10. Gu Ch. Kitaiskoe pravitel'stvo ispol'zuet razlichnye sredstva dlya bor'by s kiberterrorizmom [The Chinese government uses various means to combat cyberterrorism]. Available at: http://media.People.Com.Cn/n/2014/1120/c120837-26059821 [Accessed 15/06/17].
11. In Chen' Lin (2015). Rassmotrenie zakonodatel'stva po bor'be s terrorizmom v tselyakh uluchsheniya seti [Consideration of legislation to combat terrorism in order to improve network]. *Informatsionnaya bezopasnost' Kitaya* [Information security of China], 8, pp. 43-45.
12. Ionakh A. (1979) *Terrorizm v XXI veke: ugrozy i otvety* [The terrorism in the XXI century: threats and responses]. Boulder, Colo: Westview Press.
13. *Kontrterrorizm v Kitae neobkhodim* [Counter-terrorism in China is required]. Available at: http://www.Legaldaily.Com. /cn/commentary/content/2015-12/29/content_6423984.node=33188.Htm?Node=33188 [Accessed 14/06/17].
14. Kuin B. (2013) *Issledovanie prestuplenii sedimentatsionnogo tipa: zashchita konstitutsionnykh prav* [Study of crimes of sedimentation: protection of constitutional rights]. Pekin: Law Press.
15. Li B. (2014) Zadachi i vozmozhnosti dlya setevykh nauk v issledovanii antiterrorizma [Challenges and opportunities for network science in the study of anti-terrorism]. *Kompleksnye sistemy i nauka o slozhnostyakh* [Complex systems and the science of complexity], 1 (60).
16. Li Kh. (2015) Ugolovnoe zakonodatel'stvo v "Popravke k Ugolovnomu Kodeksu (VIIII)", svyazannoe s terrorizmom, ekstremizmom, prestupnost'yu [Criminal law in "Amendment to the Criminal Code (VIIII)" connected with terrorism, extremism, crime]. *Zhurnal Tsuchzhouskogo universiteta* [Journal of Tsuchzhousky University], 6.
17. *Narodnaya publichnaya informatsiya o bezopasnosti Kitaya* [National public information about safety in China] (2005). Pekin.

18. Ofitsial'nye dokumenty Soveta Bezopasnosti Organizatsii Ob"edinennykh Natsii [Official documents of the Security Council of the United Nations] (2014). *Sovet Bezopasnosti Organizatsii Ob"edinennykh Natsii* [Security Council of the United Nations]. Available at: http://www.fr./documents/view_doc.asp?Symbol=S/RES/2133 [Accessed 15/06/17].
19. *Organizatsiya Ob"edinennykh Natsii v bor'be s terrorizmom* [The United Nations in the fight against terrorism]. Available at: http://www.Un. Org/zh/terror/index.Shtml [Accessed 11/06/17].
20. Rezolyutsiya sovmestnoi raboty gosudarstv-chlenov po predotvrashcheniyu ispol'zovaniya terroristami tekhnologii, sredstv svyazi i resursov dlya stimulirovaniya podderzhki terroristicheskikh aktov [Resolution of joint work of member states to prevent terrorists from exploiting technology, communications and resources to encourage support for terrorist acts]. *Sovet Bezopasnosti Organizatsii Ob"edinennykh Natsii* [Security Council of the United Nations]. Available at: http://www.un.org/zh/sc/documents/resolutions/2010/s1963 [Accessed 14/06/17].
21. Sun A. (2013) Mezhdunarodnaya antiterroristicheskaya granitsa – terrorizm. Mezhdunarodnoe pravo [International antiterrorist border – terrorism. International law]. Kharbin: Kheiluntszyanskaya obrazovatel'naya pressa Publ.
22. Syaofen M., Syan Ts. (2013) Upravlenie personal'nymi dannymi: kontseptsii, tekhnologii i vyzovy [Management of personal information: concepts, technologies and challenges]. *Komp'yuternye issledovaniya i razrabotki* [Computer researches and development].
23. Tszan Ts. (2016) Obzor ugolovnogo zakonodatel'stva po bor'be s terrorizmom i "Zakon o bor'be s terrorizmom" Kitaya [Overview of the criminal legislation on terrorism and the "Law on combating terrorism" of China]. *Evraziiskii nauchnyi zhurnal* [Eurasian scientific journal], 5.
24. Veimann G. (2004) *Kak sovremennyi terrorizm ispol'zuet Internet: spetsial'nyi doklad № 116* [How modern terrorism uses the Internet: special report No. 16]. Vladivostok: Center for the Study of Organized Crime.
25. *Zhen'min' zhibao*. Available at L: http://inosmi.ru/people_com_cn/?id=236763177&date=20160604 T051721 [Accessed 18/06/17].
26. *Zhurnal Yun'nan'skogo administrativnogo kolledzha* [Journal of Yunnan Administrative College] (2012), 3.