

УДК 327.7

DOI: 10.17223/22253513/25/10

Д.С. Миц, Е.Г. Андриянченко

**АКТУАЛЬНЫЕ ВОПРОСЫ ФОРМИРОВАНИЯ СИСТЕМЫ  
ИНФОРМАЦИОННОГО ПРОТИВОДЕЙСТВИЯ  
ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ НА ТЕРРИТОРИИ  
ГОСУДАРСТВ – ЧЛЕНОВ ОДКБ**

*Рассмотрены организационно-правовые тенденции, сущность, специфика и перспективы по вопросам информационного противодействия терроризму и экстремизму на территории государств – членов ОДКБ. На основе анализа существующих доктринальных подходов, обобщения материалов научных публикаций и периодической печати, а также иных источников информационно-аналитических данных по проблеме исследования авторы раскрывают специфику формирования системы безопасности государств – членов ОДКБ в условиях новых вызовов и угроз в информационной сфере, а также формулируют обоснованные предложения по совершенствованию организационно-правовых механизмов в сфере информационного противодействия терроризму и экстремизму.*

*Ключевые слова: борьба, терроризм, информация, противодействие, экстремизм, субъект, деятельность, пространство, управление, влияние.*

СМИ и информационно-телекоммуникационные ресурсы, в том числе ресурсы сети Интернет, являются эффективным средством информационного воздействия [1] и широко используются международными террористическими и экстремистскими организациями, сторонниками этнического национализма для пропаганды экстремистской идеологии, вербовки в свои ряды новых членов, а также осуществления информационно-психологических акций в ущерб интересам безопасности государств – членов ОДКБ.

Одним из основных инструментов при реализации деструктивных замыслов экстремистского характера являются виртуальные площадки (сайты, блоги, форумы, тематические сообщества в социальных сетях), где формируются протестные сообщества, организовывается «раскрутка» информационных поводов, способных спровоцировать в обществе ситуации реальных столкновений, акций протеста и массовых беспорядков.

К числу угроз безопасности государств – членов ОДКБ, связанных с использованием информационных ресурсов и информационно-коммуникационных систем террористическими и иными экстремистскими структурами, относятся:

1. Распространение радикальных идеологий в информационном пространстве (формирование привлекательности экстремистских идеологических конструкций у социальной базы терроризма и экстремизма; панического страха перед террористами у широких слоев населения; негативного отношения к существующему государственному устройству).

2. Информационно-техническое обеспечение террористической деятельности (оправдание террористических действий и призывы к активной поддержке деятельности террористических организаций; формирование пособнической базы в социальных сетях; организация финансирования террористических и экстремистских граждан с использованием интернет-ресурсов).

3. Информационное сопровождение при планировании и организации экстремистских и террористических проявлений (насильственное изменение основ конституционного строя и нарушение целостности государств – членов ОДКБ, воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме и т.д.).

Объединяющим фактором угроз безопасности в сфере ИПТЭ является условие возможности перевода конфликтов (противоречий) любого характера в систему экстремистских и террористических проявлений.

Представители международных террористических организаций (в первую очередь МТО «Исламское государство») через социальные сети и подконтрольные им медиаресурсы оказывают негативное информационно-психологическое воздействие на различные социальные группы (прежде всего молодежь) в целях вербовки новых членов в ряды данных организаций.

Теоретические и прикладные основы организации информационного противодействия терроризму и экстремизму исследовались комплексно как единое целое во взаимосвязи всех основных элементов данной деятельности (субъект, объект, процессы, условия, результат) [2, 3]. В качестве критериев анализа научных трудов по рассматриваемой тематике выделены следующие:

- актуальность теоретико-прикладных проблем в сфере информационного противодействия терроризму и экстремизму;
- основные научные направления решения проблем в сфере информационного противодействия терроризму и экстремизму;
- сущность понятия информационного противодействия терроризму и экстремизму.

Так, с позиций философии [4–6] были рассмотрены информационные технологии как один из содержательных элементов деятельностной грани внутренней структуры современного терроризма, раскрыты содержательные аспекты экспансии терроризма в информационно-коммуникативную сферу общества, обоснованы способы противодействия терроризму с использованием информационных технологий.

В рамках социологии [7–9] исследователи уделяли особое внимание анализу проблемы терроризма в дискурсе СМИ и Интернета, а также роли и возможностям средств массовой коммуникации в борьбе с проявлениями терроризма и экстремизма.

С точки зрения политологии [10–12] были изучены причины и основные направления использования террористами современных информационных технологий в преступных целях, аспекты влияния процесса информатизации и высоких технологий на модели и формы современного терроризма, а также сущность и содержание информационного обеспечения антитеррористической деятельности государства.

Юридическое направление изучения проблемы взаимоотношений массовых коммуникаций и терроризма представлено исследованиями общих тенденций в международном и внутригосударственном праве по вопросам ограничения свободы использования СМИ в контексте борьбы с международным терроризмом. Так, Р.А. Азимов рассматривает характерные черты террористической идеологии, мотивы обращения к ней и способы формирования террористического мировоззрения. Автор обосновывает необходимость использования информационных ресурсов в целях противодействия терроризму и формирования антитеррористической идеологии в государствах – членах ОДКБ.

Процессы и условия организации деятельности в сфере ИПТЭ в диссертационных и научно-исследовательских работах охватывают широкий спектр внешних и внутренних факторов. При этом к внешним факторам, как правило, относят характеристики динамично меняющейся обстановки в сфере ИПТЭ. Как пример, существенное влияние на ее развитие оказывают следующие факторы:

- усиление влияния информации и информационных ресурсов на развитие и функционирование государственных и социальных институтов гражданского общества;

- отсутствие единого антитеррористического информационного пространства на международном и национальном уровне;

- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира;

- нарушения нормального функционирования информационных и телекоммуникационных систем (сохранность информационных ресурсов, получение несанкционированного доступа к ним), которые могут быть использованы международными террористическими организациями в своих целях;

- упрощение порядка формирования и как следствие значительное увеличение числа субъектов, осуществляющих сбор, формирование, распространение и использование информации, наличие обусловленных этим проблем осуществления контроля за легитимностью их действий;

- сохраняющиеся межэтнические, межконфессиональные и иные социальные противоречия, наличие условий для деятельности экстремистски настроенных лиц и организаций;

- ненадлежащий контроль за распространением идей радикализма, пропагандой насилия и жестокости в едином информационном пространстве государств – членов ОДКБ.

Учитывая массовую доступность информационных ресурсов, а также относительную простоту и удобство использования современных информационных технологий, практически любой субъект противоправной деятельности в той или иной степени имеет возможности использовать информационное пространство для решения собственных задач. В связи с этим актуальным представляется изучение особенностей использования информационного пространства различными субъектами террористической и

экстремистской деятельности<sup>1</sup>. К данным субъектам относятся: террористические и экстремистские организации; спецслужбы иностранных государств, поддерживающие террористические и экстремистские организации; радикальные религиозные организации и объединения; радикальные молодежные объединения; средства массовой информации, оказывающие поддержку распространению радикальных идей; зарубежные и отечественные некоммерческие неправительственные организации; радикально настроенные лидеры национальных диаспор; политические партии, представители несистемной оппозиции, которые используют радикальные методы и средства в политической борьбе.

Основными объектами, на которые направлена деятельность субъектов террористической и экстремистской деятельности в информационном пространстве, являются общественное сознание в целом, групповое сознание и социальные представления целевых аудиторий (представителей органов государственной власти и местного самоуправления, сотрудников правоохранительных органов и спецслужб, представителей общественных организаций и объединений и т.д.), а также индивидуальное сознание физических лиц. С точки зрения социологии общественное сознание представляет собой совокупность социальных представлений, чувств и настроений, господствующих в обществе в течение определенного временного интервала. Используя информационное пространство и информационные технологии, субъекты террористической и экстремистской деятельности стремятся навязать обществу социально приемлемые представления о целях и задачах экстремистских и террористических организаций, с одной стороны, а с другой – инспирировать в обществе всеобщую атмосферу фрустрации и страха перед неотвратимостью совершения террористических актов как следствие проводимой государственной политики. Тем самым субъекты террористической деятельности могут формировать предпосылки роста социально-политической напряженности в обществе.

Другим объектом негативного информационно-психологического воздействия субъектов террористической и экстремистской деятельности являются социальные представления целевых аудиторий и индивидуальное сознание физических лиц. Целевыми аудиториями являются, как правило, представители уязвимых социальных групп (национальные и религиозные меньшинства, малообеспеченные граждане, молодежь, трудовые мигранты), представители органов государственной власти и местного самоуправления, а также сотрудники правоохранительных органов. Воздействие на граждан осуществляется в целях формирования и развития устойчивой социальной базы поддержки террористических и экстремистских идей. Воздействие на органы государственной власти, местного самоуправления, а также на

---

<sup>1</sup> Под субъектами террористической и экстремистской деятельности авторы понимают не только организации и физических лиц, непосредственно осуществляющих террористическую и экстремистскую деятельность, но также тех субъектов общественного процесса, оказывающих содействие распространению радикальных идей, материальную либо иную поддержку террористическим и экстремистским организациям, а также использующим деятельность данных организаций для достижения собственных политических и экономических целей.

сотрудников правоохранительных органов осуществляется, как правило, в целях склонения их к отказу от уголовного преследования лиц, осуществляющих террористическую и экстремистскую деятельность.

В качестве средств негативного информационного воздействия субъекты террористической и экстремистской деятельности могут использовать различные средства коммуникации. Иностранные спецслужбы, иностранные неправительственные некоммерческие и международные организации, инспирирующие активность субъектов террористической и экстремистской деятельности в информационном пространстве, способны использовать любой информационный контент нейтрального характера в целях обострения социально-политических противоречий в обществе. При этом основными средствами негативного информационного воздействия субъектов террористической и экстремистской деятельности, как правило, выступают:

1. Печатная, аудио- и видеопродукция террористической и экстремистской направленности, которая используется для информирования целевой аудитории об идеологических установках террористических организаций, особенностях организации ими противоправной деятельности, а также о преследуемых террористами целях. Зачастую информационные материалы террористических организаций представляют собой программу социальных и общественных преобразований, что повышает их привлекательность и способствует увеличению числа лиц, поддерживающих взгляды данных организаций.

2. Сайты террористических и экстремистских организаций, которые являются основным средством доведения информации террористического и экстремистского содержания до целевой аудитории. Кроме того, сайты, содержащие информационные материалы террористической и экстремистской направленности, могут использоваться вербовщиками для поиска лиц, придерживающихся радикальных взглядов, в целях склонения их к ведению террористической и экстремистской деятельности либо оказанию финансовой поддержки террористических организаций<sup>1</sup>.

3. Блоги, распространяющие частные мнения и точки зрения относительно деятельности субъектов терроризма и экстремизма. Большим успехом у целевой аудитории пользуются блоги известных религиозных деятелей и представителей молодежных организаций радикальной направленности, которые предлагают радикальные методы решения социально-экономических проблем современного общества, ссылаясь на известные примеры отечественной и мировой истории. Активная блогерская деятельность данных лиц приводит к популяризации радикальных идей в отечественном информационном пространстве и способствует расширению социальной базы поддержки террористических и экстремистских идей в обществе.

4. Закрытые группы в социальных сетях и интернет-форумы, которые используются субъектами террористической и экстремистской деятельности

---

<sup>1</sup> Специальное программное обеспечение позволяет провайдеру отслеживать активность посещения сайтов, веб-страниц и иных интернет-ресурсов, а также определять персональные данные лиц, многократно посещавших данный информационный ресурс [13].

для организации общения, обмена информацией, а также в целях планирования и координации совместных действий при проведении террористических и экстремистских акций. В закрытых интернет-форумах лица могут получить необходимую информацию о способах и приемах подготовки и совершения террористических актов, изучить основы конспирации и тактики действий в случае задержания их сотрудниками правоохранительных органов, а также определить маршрут выезда на территорию, контролируемую террористами.

Кроме того, как показывает опыт «цветных революций», в период резкого обострения социально-политической обстановки в стране (регионе) социальные сети и интернет-форумы могут использоваться радикальными религиозными и общественными организациями, политическими партиями, представителями несистемной оппозиции для организации массовых беспорядков, проведения акций гражданского неповиновения и силовых акций по захвату власти в государстве. Примером тому могут служить события государственного переворота на Украине 2013–2014 гг., в ходе которого украинских граждан через форумы и социальные сети активно вовлекали в силовые акции в поддержку оппозиции.

5. Электронные письма, сообщения в социальных сетях и СМС-рассылки, содержащие предупреждения о готовящихся экстремистских акциях и террористических актах, используются субъектами террористической деятельности для создания атмосферы всеобщего страха и повышения уровня тревожности населения, связанного с угрозами их жизни и имуществу. Данные средства являются составной частью крупномасштабных информационных кампаний и направлены, с одной стороны, на создание и поддержание искусственного информационного ажиотажа вокруг проблемы терроризма, а с другой – на формирование у населения скептического отношения к деятельности собственных национальных органов безопасности и их способности противостоять существующим вызовам террористического и экстремистского характера. Кроме того, рассылка подобных информационных сообщений способствует также нагнетанию социальной напряженности в обществе, поскольку их авторы намеренно выделяют религиозную и национальную принадлежность террористов, способствуя тем самым формированию в общественной среде негативных установок по отношению к представителям определенных национальных или конфессиональных общностей.

Анализ особенностей деятельности террористических и экстремистских организаций в информационном пространстве, а также изучение объектов негативного информационно-психологического воздействия позволил определить цель деятельности субъектов терроризма и экстремизма в информационном пространстве – формирование в обществе атмосферы панического страха перед террористами, убеждений в неспособности органов власти оказывать эффективное противодействие данным угрозам (характерно для субъектов террористической деятельности) и как следствие этого – радикализация общественного сознания населения и создание очагов социально-политической напряженности на территории государств – членов ОДКБ (особенно характерно для субъектов экстремистской деятельности).

Реализация указанной цели субъектами терроризма и экстремизма в информационном пространстве сопровождается решением следующих задач:

1. Информационное сопровождение террористических и экстремистских акций. Так, на страницах сайтов, в социальных сетях или в блогах экстремистские и террористические объединения размещают информационно-пропагандистские сообщения о планируемых или совершенных действиях. При этом проведение силовых акций экстремисты обосновывают необходимостью оказания давления на репрессивные режимы с целью склонения их к переговорам с целью мирного решения возникших разногласий.

2. Организация коммуникации между субъектами террористической и экстремистской деятельности и обширной аудиторией в сети Интернет. Ряд сайтов содержит подробную информацию об экстремистских и террористических организациях, их целях и задачах, объявления о времени и месте встречи заинтересованных в поддержке террористов лиц. Большинство сайтов террористических организаций имеют версии на разных языках, что служит более широкому охвату аудитории, в том числе для воздействия на жителей других стран. В результате радикалы из любых стран или регионов мира могут находиться в тесном контакте друг с другом, обмениваться материалами, обсуждать последние новости, планировать акции, а также осуществлять иные совместные действия.

3. Привлечение граждан в ряды террористических и экстремистских организаций. Агитация в СМИ и сети Интернет со стороны террористических и экстремистских организаций приводит к тому, что пользователи в ходе посещения сайтов радикальных структур проникаются их идеями, скачивают интересующую информацию, видео- и аудиофайлы, которыми обмениваются с друзьями, знакомыми. В результате этого лица, поддерживающие радикальные идеи, могут объединяться в виртуальные сообщества с целью оказания поддержки террористическим и экстремистским организациям.

4. Обучение сторонников террористической и экстремистской деятельности в сети Интернет. Учебно-информационная работа террористических и экстремистских организаций – еще один аспект использования ими возможностей сети Интернет. В последние годы для многих экстремистских и террористических группировок Глобальная сеть стала средством подготовки новых активистов и исполнителей терактов (размещаются подробные инструкции по изготовлению взрывчатых устройств, организации засад на сотрудников правоохранительных органов и спецслужб и др.).

5. Осуществление информационной поддержки материально-технического обеспечения террористической и экстремистской деятельности. В целях привлечения дополнительных средств для финансирования террористической и экстремистской деятельности ряд, как правило, откровенно экстремистских интернет-ресурсов выступает с призывами о сборе денег. Данная деятельность обосновывается как открытым призывом о помощи террористическим и экстремистским организациям, так и под вполне благовидными предлогами. В последнее время в сети Интернет набирает популярность сбор финансовых средств на издательство религиозной

литературы, а именно – на тиражирование за счет частных пожертвований экземпляров радикальных изданий.

Таким образом, необходимо отметить, что использование информационного пространства субъектами террористической и экстремистской деятельности характеризуется стремлением субъектов террористической и экстремистской деятельности реализовать свои замыслы путем целенаправленного оказания негативного информационного воздействия на общественное сознание, формируя социальные установки на неприятие ценностей как светского общества, так и традиционных религий. При этом информационное пространство используется ими для решения задач идеологического, организационного и материального обеспечения своей противоправной деятельности.

На современном этапе в целях совершенствования системы информационного противодействия терроризму и экстремизму создается система защиты единого информационного пространства государств – членов ОДКБ, которая позволяет получать упреждающую информацию о деятельности террористических и экстремистских организаций, а также разъяснять населению ее деструктивную сущность и общественную опасность для формирования стойкого неприятия обществом идеологии насилия. В рамках создания единого антитеррористического информационного пространства [14] органам исполнительной власти предлагается активно привлекать общественные и религиозные организации, СМИ, научные и образовательные учреждения, экспертные организации, а также иные субъекты гражданского общества.

Построение системы защиты единого общегосударственного информационного пространства от террористических и экстремистских угроз осуществляется в том числе в рамках мероприятий ИПТЭ и предполагает реализацию комплекса задач при участии различных субъектов государственной власти и институтов гражданского общества. Поэтому актуальным является совершенствование механизмов координации работы между национальными органами безопасности, органами исполнительной власти и институтами гражданского общества в сфере ИПТЭ. При этом под взаимодействием национальных органов безопасности с органами исполнительной власти и институтами гражданского общества в сфере информационного противодействия экстремизму и терроризму понимается осуществляемая на единой нормативной правовой и концептуальной основе деятельность субъектов противодействия терроризму и экстремизму – уполномоченных органов государственной власти и органов местного самоуправления, в компетенцию которых входит проведение мероприятий по противодействию терроризму и экстремизму, негосударственных организаций и объединений граждан (институтов гражданского общества), а также отдельных граждан, оказывающих содействие органам государственной власти и органам местного самоуправления в осуществлении мероприятий, направленных на решение совместных задач по пресечению террористических и экстремистских действий в информационном пространстве.



Основные задачи взаимодействия национальных органов безопасности с органами исполнительной власти и институтами гражданского общества в сфере ИПТЭ включают:

- согласование мероприятий органов исполнительной власти и институтов гражданского общества по мониторингу информационной активности террористических и экстремистских организаций;
- организацию согласованного информационно-психологического воздействия со стороны органов исполнительной власти и институтов гражданского общества на целевые аудитории социальных групп, наиболее подверженных влиянию идеологий радикального толка;
- совершенствование правовой базы по координации деятельности органов исполнительной власти и институтов гражданского общества, а также организационно-методическое сопровождение в сфере ИПТЭ;
- выработку согласованных мер органов исполнительной власти и институтов гражданского общества в области профилактики терроризма и экстремизма в информационной сфере.

Полагаем, что в современных условиях активизации парламентского и экспертного (в том числе военного) межгосударственного сотрудничества рассмотренные и обоснованные в статье элементы системы ИПТЭ государств – членов ОДКБ могут быть востребованы заинтересованными экспертами при разработке, оптимизации, совершенствовании и сближении соответствующих организационно-правовых алгоритмов и механизмов национального, регионального и международного уровней.

#### *Литература*

1. *Статья 13 Доктрины информационной безопасности Российской Федерации* (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646) // Собрание законодательства РФ. 2016. 12 дек. № 50. Ст. 7074.
2. *Шкляр М.Ф.* Основы научных исследований. М.: Наука, 2008.
3. *Кокорин А.А.* Философский алгоритм познания: содержание и практические возможности. М.: Изд-во МГОУ, 2013. 322 с.
4. *Вялых В.А.* Сущность системно-деятельностного подхода [Электронный ресурс]. URL: <http://pandia.ru/text/77/450/13371>.
5. *Кафтан В.В.* Терроризм как общественное явление современности: Социально-философский анализ: дис. ... канд. филос. наук. М.: Военный университет, 2004.
6. *Резяпова Г.Ф.* Терроризм как социальное явление: дис. ... канд. филос. наук. Уфа: БГМУ, 2005.
7. *Муфтахова Ф.С.* Современный терроризм: специфика, причины, основные направления противодействия: дис. ... канд. филос. наук. Уфа: БГМУ, 2006.
8. *Никулина И.В.* Проблемы глобального терроризма в дискурсе СМИ: социологический анализ: дис. ... канд. соц. наук. Н. Новгород: НГУ им. Н.И. Лобачевского, 2007.
9. *Катрич Л.В.* Плиурализация форм терроризма в современном мире: социологические подходы: дис. ... канд. соц. наук. М.: МГИМО, 2009.
10. *Гурба В.Н.* Терроризм в регионах адатных культур: на примере Северо-Кавказского региона: дис. ... д-ра соц. наук. Новочеркасск: ЮРГТУ, 2011.
11. *Соломин Д.А.* Противодействие терроризму в информационной сфере: дис. ... канд. полит. наук. М.: Дип. академия, 2004.
12. *Шамов М.И.* Государственная стратегия и политические технологии предупреждения информационного терроризма в современном российском обществе: дис. ... канд. полит. наук. Н. Новгород: НГУ им. Н.И. Лобачевского, 2007.

13. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем. Т. 1: Угрозы, уязвимости, атаки и подходы к защите. М.: Телеком, 2006. С. 44–48.

14. Концепция противодействия терроризму в Российской Федерации (утв. Президентом Российской Федерации 5 октября 2009 г.) // Российская газета. 2009. 20 окт. № 198.

*Mits Denis S.* Advisory Board of the Council of the Parliamentary Assembly of the Collective Security Treaty, Joint Commission of the IPA CIS on the harmonization of legislation in the sphere of security and counteraction against new challenges and threats,

*Andryjanchenko Eugene G.* Moscow Institute of Radioengineering, electronics and automation (Moscow, Russian Federation)

### **TOPICAL ISSUES OF FORMATION OF THE SYSTEM OF INFORMATIONAL COUNTERACTION TO TERRORISM AND EXTREMISM ON THE TERRITORY MEMBER STATES OF THE CSTO**

Keywords: battle, terrorism, information, resistance, extremism, entity, activity, space, control, influence.

The article considers the legal trends, the essence, specificity and prospects of informational counteraction to terrorism and extremism on the territory of the member States of the CSTO. The author defines the main directions of cooperation between national security agencies with the Executive bodies, civil society institutions and individual citizens on the protection of information space from illegal encroachments of subjects of terrorist and extremist activities.

The results of the analysis of scientific works in which substantial aspects of informational counteraction to terrorism and extremism were discussed from different perspectives (philosophical, political, sociological and legal), revealed a theoretical and applied basis for the organization of informational counteraction to terrorism and extremism on the territory of the member States of the CSTO. On the basis of studying the characteristics of the activities of terrorist and extremist organizations in the information space for the Russian segment of the Internet was identified the main threats to the security of States – CSTO members related to the use of information resources and information and communication systems by terrorists and extremists; classified subjects, the possibility of using the Internet to organize and support their illegal activities; defined the main objects of the negative impact of terrorist and extremist organizations, with the help of modern information technologies.

The authors believe that the main objectives of terrorists and their accomplices in the information space are: the organization of communication between subjects of terrorist and extremist activities and a vast audience on the Internet; involvement of citizens into the ranks of terrorist and extremist organizations; training of supporters of terrorist and extremist activities on the Internet; provision of information support of terrorist and extremist activities. In General, these entities aim to create in society an atmosphere of fear terrorists, to form beliefs in the inability of the authorities to provide effective counteraction to these threats and as a consequence – to radicalize the public consciousness of the population and to create pockets of socio-political tension in the territory of the member States of the CSTO.

To successfully counteract these threats, the authors propose to organize a system of protecting a single national information space from terrorist and extremist threats, which involves the implementation of measures, IPTA with the participation of different actors of state and civil society institutions.

### *References*

1. President of the Russian Federation. (2016) Stat'ya 13 Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii (utv. Ukazom Prezidenta Rossiyskoy Federatsii ot 5 dekabrya 2016 goda № 646) [Article 13 of the Doctrine of Information Security of the Russian Federation (approved by Decree No. 646 of the President of the Russian Federation of December 5, 2016)]. *Legislative Bulletin of the Russian Federation*. 50. Art. 7074.

2. Shklyar, M.F. (2008) *Osnovy nauchnykh issledovaniy* [Fundamentals of Scientific Research]. Moscow: Nauka.

3. Kokorin, A.A. (2013) *Filosofskiy algoritm poznaniya: sodержanie i prakticheskie vozmozhnosti* [Philosophical Algorithm of Cognition: Content and Practical Possibilities]. Moscow: Moscow State Regional University.

4. Vyalykh, V.A. (n.d.) *Sushchnost' sistemno-deyatel'nostnogo podkhoda* [Essence of the System-Activity Approach]. [Online] Available from: <http://pandia.ru/text/77/450/13371>.
5. Kaftan, V.V. (2004) *Terrorizm kak obshchestvennoe yavlenie sovremennosti: Sotsial'no-filosofskiy analiz* [Terrorism as a Social Phenomenon of Our Time: Socio-Philosophical Analysis]. Philosophy Cand. Diss. Moscow: Voenny universitet.
6. Rezyapova, G.F. (2005) *Terrorizm kak sotsial'noe yavlenie* [Terrorism as a social phenomenon]. Philosophy Cand. Diss. Ufa: Bashkir State Medical University.
7. Muftakhova, F.S. (2006) *Sovremennyy terrorizm: spetsifika, prichiny, osnovnye napravleniya protivodeystviya* [Modern Terrorism: Specificity, Causes, Main Directions of Counteraction]. Philosophy Cand. Diss. Ufa: Bashkir State Medical University.
8. Nikulina, I.V. (2007) *Problemy global'nogo terrorizma v diskurse SMI: sotsiologicheskii analiz* [Problems of Global Terrorism in the Discourse of the Media: Sociological Analysis]. Sociology Cand. Diss. Nizhny Novgorod.
9. Katrich, L.V. (2009) *Pluralizatsiya form terrorizma v sovremennom mire: sotsiologicheskie podkhody* [The Pluralization of Forms of Terrorism in the Modern World: Sociological Approaches]. Sociology Cand. Diss. Moscow: Moscow State Institute of International Relations.
10. Gurba, V.N. (2011) *Terrorizm v regionakh adatnykh kul'tur: na primere Severo-Kavkazskogo regiona* [Terrorism in the regions of adat cultures: a case study of the North Caucasus region]. Sociology Dr. Diss. Novocherkassk.
11. Solomin, D.A. (2004) *Protivodeystvie terrorizmu v informatsionnoy sfere* [Counteraction to terrorism in the information sphere]. Political Studies Cand. Diss. Moscow.
12. Shamov, M.I. (2007) *Gosudarstvennaya strategiya i politicheskie tekhnologii preduprezheniya informatsionnogo terrorizma v sovremennom rossiyskom obshchestve* [State strategy and political technologies for the prevention of information terrorism in modern Russian society]. Political Studies Cand. Diss. Nizhny Novgorod.
13. Zapechnikov, S.V., Miloslavskaya, N.G., Tolstoy, A.I. & Ushakov, D.V. (2006) *Informatsionnaya bezopasnost' otkrytykh system* [Information Security of Open Systems]. Vol. 1. Moscow: Telekom. pp. 44–48.
14. President of the Russian Federation. (2009) *Kontseptsiya protivodeystviya terrorizmu v Rossiyskoy Federatsii* (utv. Prezidentom Rossiyskoy Federatsii 5 oktyabrya 2009 g.) [The concept of countering terrorism in the Russian Federation (approved by the President of the Russian Federation on October 5, 2009)]. *Rossiyskaya gazeta*. 20th October.