Современный этап мирового развития характеризуется тем, что собственно информация, средства информатизации и связи, а также общественные отношения, складывающиеся в процессе сбора, обработки, хранения, передачи и распространения информации оказывают непосредственное и все более возрастающее влияние на экономическое, социальное и духовное развитие как отдельных государств, так и мирового сообщества в целом. Это свидетельствует о том, что в современных условиях информация и управление ею становится основанием и главным инструментом достижения целей в новом мироустройстве. Официально об этом было заявлено 22 июля 2000 года в Японии в ходе подписания руководителями восьми ведущих стран мира «Окинавской хартии глобального информационного общества». В этом документе продекларировано, что «информационно-телекоммуникационные технологии стали одним из наиболее важных факторов, влияющих на формирование общества XXI века.

Таким образом, на официальном уровне заявлено о вступлении мировой цивилизации в период своего развития, получившего название «информационного общества». По данным ЮНЕСКО объем современного рынка информационных услуг и технологий в настоящее время превышает 2 трлн. долларов и составляет 15% мировой торговли. В России только объемы реализации средств вычислительной техники и информатики оценивается более, чем в 1,5 млрд. долларов в год, а с учётом продаж программного продукта – около 4,5 млрд. долларов, что составляет около 5% годового ВВП России.

Наряду с очевидными благами мировая информационно-технологическая революция создала принципиально новые потенциальные угрозы жизнедеятельности как отдельных обществ, государств и их граждан, так и мирового сообщества в целом. В наибольшей степени это касается терроризма, мутация которого, по мнению специалистов, в наибольшей степени происходят именно в информационной сфере.

Быстрое развитие новых технологий существенно расширило возможности террористических организаций по манипулированию сознанием населения при подготовке и проведении террористических акций.

В связи с этим следует подчеркнуть такие характеристики современного терроризма:

* нацеленность на получение сильного эмоционального эффекта от своих действий в обществе. Это выражается посредством достижения состояния страха и неуверенности у атакуемого населения и стремления к одобрению и симпатиям у своих последователей;
* ориентация на распространение информации о совершённом теракте среди широкой общественности;
* атаки производятся на такие объекты, которые имеют особый символический смысл для общества;
* применение насилия террористами воспринимается в обществе (в первую очередь в развитых странах) как противоестественное, вступает в конфликт с социальными нормами и порождает в результате чувство тревоги, неуверенности и неизвестности.

При этом информационно-подрывная деятельность террористов может носить явный характер, и проводиться ими открыто или осуществляться скрытно, вестись от имени антитеррористических сил либо анонимно.

Основная цель террористов состоит в том, чтобы террористический акт стал известен населению и органам власти, получил широкий общественный резонанс. Такой общественный резонанс порождает страх и панические настроения среди членов общества, приводит к потере доверия к власти, и в конечном итоге вызывает политическую нестабильность.

Исходя из этого можно сделать вывод о наличии особой ***информационно-коммуникативной стратегии*** терроризма, которая и отличает его от каких-либо иных повстанческих или диверсионных действий. Посредством подобной стратегии террористические организации демонстрируют свою способность воздействия на органы государственной власти. Достигаемый эффект в значительной степени зависит:

* от возможностей и особенностей функционирования в конкретном обществе каналов коммуникации;
* от характера появляющихся в средствах массовой информации сообщений;
* от способности СМИ представить случившееся как сенсацию.

Серьезную опасность представляет стремление международных террористических организаций использовать СМИ в качестве инструмента достижения своих преступных целей. У современного террора полем боя становится телеэкран. И не случайно в своих акциях террористы прежде всего требуют не денег, а ставят политические цели, требуют телекамеру и тележурналистов. Цель – манипулирующее воздействие на общество, чтобы уже оно предъявляло ультиматум своим лидерам.

Как показывает практика, информационный терроризм направлен не только на нанесение ущерба интересам отдельных государств, но и на расширение политического, экономического, идеологического влияния международных террористических организаций в мировом сообществе.

Развитие трансграничных электронных СМИ существенно расширяет возможности международных террористических организаций по манипулированию массовым сознанием. Такое, манипулирование, имея «мишенью» население нацеливается на изменение его сознания и поведения в выгодную для террористов сторону. При этом недостаточная информационная культура определенной части населения, слабая защищенность его от влияния экстремистской идеологии приводят к тому, что манипулируемые часто не сознают, что их мировоззрение идеалы, ценности, потребности и в целом образ мыслей во многом определяются антиобщественными интересами тех, кто ими манипулирует и стремится к господству над их духовным миром.

Современный информационный арсенал террористов насчитывает сотни приемов манипулирования с использованием СМИ, каналов межличностной, личностно-групповой и межгрупповой коммуникации. Информационно-террористическая деятельность все чаще приобретает скрытый, изощренный, заказной и долговременный характер, хорошо обеспечивается материально, ее способы и методы постоянно оттачиваются и совершенствуются от одного террористического акта к другому.

Особую озабоченность вызывает возможность использования террористами новых и нетрадиционных информационных технологий для оказания скрытого информационно-манипулятивного воздействия на сознание и деятельность людей. Так, в частности, отличительной особенностью реализации информационно-коммуникативной стратегии терроризма является активное использование возможностей глобальной сети Интернет.

Относительная дешевизна, простота и доступность современных средств информации позволяют террористам проводить свои преступные акции, находясь на значительно «безопасном» расстоянии от объекта терроризма, оставаться довольно длительное время безнаказанными. При этом наносится значительный материальный и моральный ущерб обществу, государству, личности.

Как показывает практика Интернет, электронная почта, системы цифровой телефонной радиосвязи обеспечивают экстремистам не только более широкие возможности для взаимодействия и пропаганды своих идей, но также для ведения информационных войн.

Об этом в частности свидетельствует появление нового вида преступной деятельности, получившей название «сетевая война» (netwar). Вести ее могут небольшие группы специально подготовленных кибертеррористов и даже одиночки географически отдаленные друг от друга, но тайно общающиеся между собой в «сетевом» формате. Теоретической основой такой деятельности является концепция «сопротивление без руководства», лидера американской радикальной организации «Крайние правые» Л. Бим. Согласно этой концепции все члены группы («ячейки-фантомы») действуют независимо друг от друга и никогда не обращаются в центральную штаб-квартиру или к лидерам за указаниями. Предполагается, что они сами обязаны знать, что и как делать, реагируя на конкретные события. Информационную же подпитку они получают через анонимно распространяемые электронные бюллетени и страницы в Интернете. Указанная форма организации, получившая название networking помогает экстремистам находить союзников, реализовывать свое влияние, а также осуществлять управление проводимыми операциями.

Все это свидетельствует о том, что наблюдаемое в последнее время усиление влияния информационных технологий практически на все сферы жизнедеятельности человечества выдвигают задачу информационного противодействия в разряд основных задач борьбы с терроризмом.

Между тем современные реалии свидетельствуют о том, что информационное противодействие является одним из наименее разработанных направлений антитеррористической деятельности как на уровне международного сотрудничества, так и непосредственно в Российской Федерации.

Более того, само понятие «информационное противодействие» вплоть до настоящего времени не получило своего терминологического определения. По крайней мере, в официальных источниках сущность и содержание информационного противодействия терроризму не определены.

На практике же информационный аспект борьбы с терроризмом предполагает лишь реализацию мер защитного характера. Реализация активных мер информационного противодействия угрозам терроризма в официальных документах не предусматривается.

Так, в Доктрине информационной безопасности, утвержденной Президентом Российской Федерации 9 сентября 2000 года № Пр-1895 данное направление предполагает только лишь предотвращение несанкционированного доступа «…к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом…».

В Федеральном законе Российской Федерации от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму» информационное противодействие предполагается только лишь в рамках статьи 11, определяющей правовой режим контртеррористической операции.

Таким образом, деятельность органов безопасности Российской Федерации по информационному противодействию терроризму предполагается только после совершения теракта и не предусматривает активных предупредительных мер. В этом на наш взгляд уязвимость существующий в Российской Федерации системы информационного противодействия терроризму, поскольку информационное воздействие терроризма носит, как показывает анализ, именно наступательный характер.

Не нашло своего отражения информационное противодействие терроризму и в новой редакции модельного закона СНГ «О борьбе с терроризмом» (Постановление Межпарламентской Ассамблеи государств − участников Содружества Независимых Государств от 17 апреля 2004 года № 23-5). Новеллой данного закона является глава 3 «Информационно-пропагандистское обеспечение борьбы с терроризмом». Несмотря на своё название, глава содержит лишь нормы регламентирующие деятельность СМИ по содействию в борьбе с терроризмом, а также меры профилактики терроризма с использованием средств массовой информации. Статья 9 данного закона определяет ответственность средств массовой информации за нарушения в части содействия борьбе с терроризмом.

Закон, таким образом, не предусматривает ни противодействия информационному терроризму, ни использование информационных технологий в борьбе с терроризмом.

К этому следует добавить также и тот факт, что Российская Федерация в силу ряда обстоятельств вплоть до настоящего времени не присоединилась к Конвенции Совета Европы о киберпреступности, направленной на борьбу с преступлениями в сфере компьютерной информации.

В целом, как показывает анализ, в Российской Федерации вплоть до настоящего времени нормативно-правовая база, регламентирующая информационное противодействие терроризму, особенно с использованием информационных технологий не разработана.

Исключение в этом плане представляют лишь ведомственные нормативные акты правоохранительных органов, осуществляющих борьбу с терроризмом (Министерства внутренних дел, Федеральной службы безопасности и Национального антитеррористического комитета). Таким образом, само информационное противодействие терроризму носит ведомственный характер.

На основе анализа реальной политической практики представляется возможным определить информационное противодействие терроризму как комплекс мероприятий по поражению информационного ресурса террористических организаций, блокированию осуществляемых ими информационных процессов и внедрению дезинформации на всех этапах их реализации.

Сущность информационного противодействие терроризму заключается в обеспечении достижения целей государственной антитеррористической политики путем применения специальных средств и способов воздействия на информационный ресурс террористических структур, а также осуществление защиты и эффективного использования собственного информационного ресурса.

В содержательном аспекте информационное противодействие терроризму предполагает реализацию комплекса мер, основными из которых, по мнению отечественных специалистов являются:

* противодействие идеологии терроризма, сепаратизма, национализма, религиозного экстремизма;
* информационное обеспечение контртеррористической деятельности через средства массовой информации и другие информационные каналы;
* прогнозирование террористической угрозы, источников ее формирования и развития, а также условий реализации;
* поиск, сбор, добывание и анализ оперативной информации о действиях террористических организаций и их пособников;
* четкое информационное взаимодействие между субъектами контртеррористической деятельности и надежное обеспечение защиты оперативной информации;
* информационная работа с местным населением, формирование бдительности, морально-психологической устойчивости, сплоченности, дисциплинированности и личной ответственности;
* обучение населения правилам поведения в условиях возрастания террористической угрозы, в случаях террористических акций, своевременная первая помощь, материальная и моральная поддержка лиц, пострадавших от террористов;
* информационное воздействие на сознание террористов, их пособников, организаторов и вдохновителей, на международные террористические организации;
* создание организационных, правовых, научных, технических, кадровых, финансовых и других благоприятных условий для эффективного информационного обеспечения контртеррористической деятельности.

В настоящее время систему информационного противодействия терроризму в РФ составляют соответствующие структуры Федеральной службы безопасности, Министерства внутренних дел и ряда других структур.

Наиболее целенаправленно деятельность по информационному противодействию терроризму осуществляется Национальным антитеррористическим комитетом.

Так, по материалам открытой печати в рамках разработанной Национальным антитеррористическим комитетом федеральной целевой программы «Антитеррор 2008 – 2012» предполагается реализовать более семидесяти мероприятий, цель которых – создание учебной базы для подготовки специалистов антитеррористических подразделений, формирование единой информационной среды, а также ввод в эксплуатацию новых технических средств выявления и пресечения террористической деятельности.

Важнейшим направлением информационного противодействия международному терроризму является развитие сотрудничества государств СНГ, других региональных организаций и ООН.

Так, в рамках Антитеррористического центра (АТЦ) СНГ в целях накопления, обобщения и систематизации информации в сфере борьбы с терроризмом, а также повышения межгосударственного информационного взаимодействия создана и эксплуатируется межгосударственная автоматизированная информационная система – Специализированный банк данных АТЦ СНГ. Тематический перечень накапливаемых в нем сведений, определенный Положением об АТЦ СНГ, первоначально включал информацию о международных террористических и иных экстремистских организациях, их лидерах, причастных к ним лицах; состоянии, динамике и тенденциях распространения международного терроризма, а также о неправительственных структурах и лицах, оказывающих поддержку международным террористам.

По мере развития Специализированного банка данных, с учетом расширения и уточнения приоритетных направлений деятельности Центра сформирован ряд тематических информационных массивов. В их числе массивы, содержащие сведения в отношении лиц, объявленных в международный розыск по подозрению в совершении преступлений террористического характера; юридических и физических лиц, финансирующих террористические и экстремистские организации; лиц и организаций, подозреваемых в причастности к совершению актов терроризма с использованием террористов-смертников.

Реальным вкладом в развитие международного анти террористического взаимодействия является разработка Антитеррористическим центром СНГ концепции сотрудничества органов безопасности и спецслужб в сфере информационного противодействия терроризму и экстремизму. В рамках данной концепции Антитеррористическим центром СНГ реализуется комплекс мер, направленных на создание единого правового поля в сфере информационного противодействия терроризму.

Информационное противодействие терроризму является одним из приоритетных направлений деятельности ОДКБ. Реализуемые в данной области мероприятия предполагают содействие становлению и укреплению потенциала коллективного информационного противодействия террору, наркоугрозе и другим вызовам на пространстве ОДКБ.

С этой целью Организация наращивает международные связи, находит сторонников и союзников в наиболее влиятельных СМИ, привлекает к сотрудничеству писателей, ученых, деятелей культуры, организует работу так, чтобы на экранах и печатных полосах появлялись правдивые материалы контртеррористической, антинаркотической тематики, против экстремизма и идеологии насилия.

В рамках Целевой программы предусмотрено создание в формате ОДКБ Совета по координации информационной политики, который формировал бы приоритетные направления совместной работы. Предполагается, что это будет вспомогательный орган при ОДКБ, который при должной инициативе и активности его участников мог бы стать важным компонентом в работе по реализации целей и задач ОДКБ и, прежде всего, по антитеррору.

Таким образом, информационное противодействие терроризму, осуществляемое в Российской Федерации и региональных структурах СНГ предполагает комплексную реализацию системы мер по профилактике и предупреждению терроризма посредством сбора и анализа информации о террористических структурах и их нейтрализации посредством использования информационных ресурсов, прежде всего с помощью СМИ.

Зарубежный опыт информационного противодействия терроризму несколько отличается от российского.

Так, например, в США информационное противодействие терроризму реализуется посредством информационных операций, под которыми понимаются «действия, направленные на достижение информационного превосходства путем воздействия на информацию противника, основанные на информации процессы, информационные системы и компьютерные сети, и принятие мер по защите собственной информации».

В зависимости от объектов воздействия информационные операции наступательного характера западные специалисты подразделяют на три основных вида:

* нападение на инфраструктуры противника в целях нанесения ущерба накопленной информации или информационным системам;
* дезинформация противника путем манипулирования фактами (их искажение или фальсификация), с тем, чтобы вынудить его осуществлять действия не соответствующие его интересам;
* оказание влияния на волю и настроения (психологические операции) общества в целом, его отдельных групп или индивидов, с тем, чтобы вызвать страх, породить раскол или брожение, а также другие негативные явления.

Последние два вида информационных операций считаются наиболее приемлемыми в борьбе с международным терроризмом. Психологическое воздействие на население позволяет внушить обществу отрицательное отношение к фанатизму, насилию, расизму и т. д., что лишает террористов поддержки, ограничивает их возможности в вербовке пополнения и добывания финансовых средств.

Особым направлением информационного противодействия терроризму в США и ряде западных стран является использование информационных технологий.

Например, еще в июне 2004 года руководители американского, британского и австралийского антитеррористических центров объявили о намерении создать единую информационную сеть, которая, «позволит предотвращать акции Аль-Каиды и союзных с ней формирований на всей территории земного шара». Основным направлением работы этой сети должно стать максимальное информационное покрытие всех потенциально опасных зон и регионов мира и непрерывная циркуляция данных о предполагаемых терактах или перемещениях террористов для оперативного принятия компетентными службами соответствующих мер.

В результате была создана структура, которая полностью повторяла систему глобального радиоперехвата ECHELON времен мировой войны. Участниками современной глобальной антитеррористической сети являются: в США – Национальный контртеррористический цент, В Великобритании – Объединенный Центр анализа терроризма, в Австралии – Национальный центр распределения угроз, в Канаде – Объединенный центр распределения угроз, в Новой Зеландии – Совместная группа распределения угроз.

Кроме структуры и состава участников, создатели глобальной антитеррористической сети взяли у ECHELON еще одну идею – создание единой технологической площадки для взаимного обмена информацией.

Так, по оценкам западных специалистов, только на каналах мобильной и стационарной телефонной связи эта система ежегодно перехватывает по всему миру и обрабатывает не менее 4 млрд. переговоров.

Сформированная глобальная антитеррористическая сеть используется также для перехвата и обработки информации, в том числе зашифрованной, циркулирующей в системах высокоскоростной кабельной связи в подземном, наземном и подводном исполнении. Важным направлением использования системы в борьбе против терроризма является фильтрация и обработка сообщений электронной почты и файлов, передаваемых через сеть Интернет. Что касается обработки файлов, передаваемых через сеть особенно цифровых фотографий и другой графики, то средствами системы ECHELON осуществляется их сканирование и статистический анализ на наличие стенограмм, которыми потенциально могут пользоваться террористические организации для скрытой передачи зашифрованных конфиденциальных данных. В случае обнаружения закамуфлированных криптограмм производится их расшифровка с использованием имеющихся программных средств.

Таким образом, анализ существующей практики и тенденций развития информационного противодействия терроризму свидетельствует о различных подходах к предотвращению и нейтрализации угроз терроризма. Эффективное решение этой задачи требует координации усилий, базирующихся на общедоступном обмене информации, о достижениях в области информационной безопасности как отдельных государств, так и мирового сообщества в целом. Это обусловлено тем, что современная глобализация предполагает и глобализацию терроризма, выход его на транснациональный (международный) уровень и соответственно глобализацию информационного противодействия ему.