Тема: « Информационный терроризм в современном мире »

**Содержание**

**Введение**3

**Глава 1. Эволюция терроризма в информационную эпоху**

§ 1. Терроризм: феноменология явления 7

§ 2. Тенденции информационной эры 8

§ 3. Масштаб угрозы 15

**Глава 2. Информационный терроризм: технологии воздействия**

§ 1 Информационные технологии как инструмент влияния 21

§ 2. Средства информационного оружия 27

§ 3. Информационное насилие 36

§ 4. Искусство “формировать реальность” 49

**Глава 3. Противодействие информационным угрозам**

§ 1. Минимально необходимые действия Правительства 54

§ 2. Аспекты создания целостной системы информационной безопасности 58

**Заключение**68

**Список использованной литературы**73

**Введение**

Сегодня проблема информационного терроризма начинает привлекать все больше внимания в современной политической науке. Это связано, в первую очередь, с постоянно ускоряющимся техническим прогрессом, нарастающей информатизацией общества и переходом мировой цивилизации в информационную эпоху. Современное общество немыслимо без коммуникаций, вся жизнь среднего европейца, американца, да и уже многих россиян плотно “завязана” на информации. Нарушение работы информационных систем неизбежно влечет за собой потерю чувства реальности, хаос, как общественный, так и экономический упадок. Рассматривая роль массовых коммуникаций и их влияние на политические процессы, российские политологи отмечают, что в постиндустриальном обществе власть знаний и информации становится решающей в управлении обществом, оттесняя на второй план влияние денег и государственного принуждения. Причем непосредственными носителями и, особенно, распространителями знаний и другой социально значимой информации являются средства массовой коммуникации[[1]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn1) .

**Глава 1. Эволюция терроризма в информационную эпоху**

**§ 1. Терроризм: феноменология явления**

Когда мы приступаем к рассмотрению того или иного социального явления, то нас интересует, прежде всего, его отличительные признаки, которые позволяют выделить данное явление из ряда других, пусть близких, но все-таки не тождественных. В первую очередь мы пытаемся дать определение рассматриваемому явлению. То же самое происходит и при анализе терроризма. Сделать это не просто, так как явление имеет очень сложную структуру. Терроризм является нам под различными масками, часть из которых, на первый взгляд, абсолютно не связаны с ним. Причем это явление настолько многогранное, что в нем соседствуют и идеологические, и религиозные, и этнические, и многие другие компоненты. Они настолько переплетаются друг с другом, что дать точный ответ на вопрос: “С каким видом терроризма мы имеем дело?” - бывает весьма затруднительно.

Кроме того, генезис данного явления свидетельствует о его значительной трансформации: изменяются формы осуществления террористических актов, происходит смещение в поле целевого воздействия террористов, меняются методы их работы, особенности организационного строительства и многое другое. Также, терроризм имеет много общего с другими формами социального протеста и насилия: агрессией, вооруженной борьбой, военными конфликтами различной степени интенсивности, партизанскими действиями, диверсиями и др. Поэтому вполне понятно то обилие определений, которое на сегодняшний день предлагается исследователями.

В современной западной литературе существует свыше ста определений терроризма[[5]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn5) . “Терроризм, - отмечают А.В. Змеевский и В.Е. Тарабрин, - явление весьма сложное, динамичное и многоплановое. Помимо правовых он затрагивает и целый ряд других проблем - психологические, исторические, технологические и т.д. Не случайно международному сообществу так и не удалось выработать общеприемлемое юридическое определение терроризма, хотя сущностное наполнение этого феномена для всех понятно. Здесь присутствует и противозаконное насилие, как правило, с применением оружия, и стремление запугать широкие слои населения, и невинные жертвы, а применительно к террористическим актам, выходящим за рамки государственных границ, - международный элемент”[[6]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn6) .

Зарубежные исследователи терроризма также подчеркивают, что это явление легче описать, чем дать ему четкое, однозначное толкование. Именно так поступает американский исследователь Б. Дженкинс при трактовке данного понятия. “Терроризм, - подчеркивает он, - определяется в зависимости от характера акции, а не от личности исполнителя или сути дела, за которое он борется. Все террористические акции сопряжены с применением насилия или угрозой насилия, часто это сопровождается выдвижением конкретных требований. Насилие направлено в основном против гражданских объектов. Мотивы имеют политический характер. Акции совершаются так, чтобы привлечь максимум общественного внимания. Исполнители, как правило, являются членами организованных групп или, в отличие от других преступников, берут на себя ответственность за совершаемые акции. И, наконец, сама акция призвана оказать воздействие, выходящее за рамки причинения непосредственного физического ущерба”[[7]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn7) .

В федеральном законе РФ “О борьбе с терроризмом” указывается, что терроризм представляет собой “насилие или угрозу его применения в отношении физических лиц или организаций, а также уничтожение (повреждение) или угрозу уничтожения (повреждения) имущества и других материальных объектов, создающую опасность гибели людей, причинения значительного ущерба, либо наступления иных общественно-опасных последствий, осуществляемых в целях нарушения общественной безопасности, устрашения населения или оказания воздействия на принятие органами власти решений, выгодных террористам.”

**§ 2. Тенденции информационной эры**

Современная цивилизация вступила в эпоху, которую Элвин Тоффлер охарактеризовал как информационное общество, где главным фактором общественного развития является производство и использование информации. Информационный сектор экономики, следующий за сельским хозяйством, промышленностью и экономикой услуг, занимает доминирующее место в этом новом обществе. В связи с этим вся история человеческой цивилизации может быть осмыслена через способ сбора, производства, анализа, использования информации и управления информационными процессами в обществе[[8]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn8) . И тогда она предстает в виде стадий, каждая из которых тесно взаимосвязана со сменой способов воспроизводства информации, вызванных эволюционной или революционной сменой технологического базиса воспроизводства обществом информации. Всего можно выделить пять эволюционно-информационных стадий развития человеческой цивилизации, обусловленных соответствующими типами информационных технологий.

Первая (устно-речевая) информационная технология, связанная с возникновением осмысленной речи и языка как общепринятого средства коммуникативного общения между людьми в обществе, - языковая или речевая технология передачи и воспроизводства информации. Информация передается с помощью простой речи, а языковыми носителями являются сами живые люди.

Вторая (письменная) информационная технология, связанная с возникновением письменности и грамматических правил, - письменная технология передачи и воспроизводства информации. Информация передается с помощью знаковых носителей (символы, сигналы, знаки, рукописи).

Третья (книгопечатная), связанная с возникновением книгопечатания, - книжная технология передачи и воспроизводства информации. Информация передается с помощью книжных носителей (письма, книги).

Четвертая (радио-телеграфная) - связана с возникновением разнообразных электромагнитных технологий передачи и воспроизводства информации. Информация передается с помощью различного рода электромагнитных сигналов, преобразующихся в зрительно-звуковые символы по телеграфу, телефону, радио, телевидению. Это существенно изменило стандарты скорости и объемов передачи, обработки, производства и накопления информации в обществе.

Пятая (компьютерная), связанная с возникновением и распространением компьютерных технологий передачи и воспроизводства информации. Информация передается, обрабатывается и воспроизводится с помощью ЭВМ и компьютеров, создаются всемирные компьютерные, телекоммуникационные и космические сети связи и передачи информации. Все это обусловило революционный переворот в способах обработки и передачи больших объемов информации. На этом этапе можно говорить о вступлении человеческой цивилизации в начальную фазу информационного общества, начале информатизации человечества. О том, что вместе с добропорядочными людьми туда вступают и террористы, свидетельствуют факты.

Так, в 1997 году араб-компьютерщик Халил Дик, натурализовавшийся в США, но родившийся на оккупированных Израилем палестинских территориях, выехал в Пакистан, чтобы сохранить на компакт-диске для потомков некий труд великого мусульманского религиозного деятеля. 16 декабря 1999 года его выдворили из Пакистана и арестовали в Иордании вместе с тринадцатью сообщниками, замешанными в подготовке терактов перед празднованием Миллениума. Компакт-диск, который полиция конфисковала в доме Халила Дика в Пакистане недалеко от афганской границы после его ареста в Иордании, оказался вовсе не трудом великого мусульманского религиозного деятеля. Оказалось, что на компакт-диске, найденном у Дика, содержатся тысячи пронумерованных отсканированных страниц на арабском языке, составляющих настоящую энциклопедию терроризма.

В одном из томов, посвященном взрывчатым веществам, рассказывалось о различных видах противотанковых мин и гранат и о том, как их использовать на поле боя. Закладка тротиловых зарядов или пластида, одного из самых любимых террористами видов взрывчатого вещества, являлось сюжетом другого, весьма детализированного учебника. В третьем пособии рассказывалось об уходе за личным и штурмовым оружием и его применении в уличных боях. В остальных речь шла о первой помощи при огнестрельных или осколочных ранениях при подрыве на пехотных минах и о кустарном изготовлении - от приклада до прицела - автоматического оружия. На большом количестве рисунков курсанты могли обучаться азам терроризма. Связь Халила Дика с Усамой бен Ладеном почти не вызывала сомнений. Действительно, было быстро и без особого труда установлено, что в Пакистане у американца был общий банковский счет с Абу Зубайдом, одним из помощников бен Ладена.

По прогнозу японских ученых, до 2007 года человечество будет находиться в условиях кибернетической революции. Затем будут весьма эффективно развиваться биоэнергология и биоинформатика. Именно тогда, по их прогнозам, в рамках компьютерной стадии общество будет работать в направлении создания невещественных цифровых квантово-полевых технологий передачи и воспроизводства информации (например, биоквантовых компьютеров, соединенных со своими персонифицированными носителями и объединенных в глобальную биоквантово-полевую сеть), что может позволить сформировать и развивать глобальную всемирную компьютерно-телекоммуникационную биоквантово-полевую и цифровую суперсеть по сбору; обработке, производству, накоплению, использованию информации во всем мире и во всех сферах жизни человеческого общества, а также позволит в определенной мере осуществлять глобальное управление индивидами и глобальный контроль за происходящими в обществе информационными процессами. Но это - в будущем.

Однако уже на современном этапе развития цивилизации информация стала играть ключевую роль в функционировании общественных и государственных институтов и в жизни каждого человека. На наших глазах процесс информатизации развивается стремительно и зачастую, непредсказуемо, и мы лишь начинаем осознавать его социальные, политические, экономические, культурологические, военные и другие последствия. Информатизация ведет к созданию единого мирового информационного пространства, в рамках которого производится накопление, обработка, хранение и обмен информацией между субъектами этого пространства - людьми, организациями, государствами. Вполне очевидно, что возможности быстрого обмена политической, экономической, духовной, научно-технической и другой информацией, применение новых информационных технологий во всех сферах общественной жизни, и особенно в производстве и управлении, является несомненным благом. Но подобно тому, как быстрый промышленный рост создал угрозу экологии Земли, а успехи ядерной физики породили в свое время опасность ядерной войны, так и информатизация становится источником целого ряда проблем, в том числе и информационного терроризма.

Этот новый вид терроризма реализуется в некой “инфосфере”, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Данная сфера имеет существенные особенности, которые кардинально отличают ее от других компонентов среды обитания человека: неисчерпаемость и восполняемость инфоресурсов, возможность их быстрого копирования, перемещения больших объемов практически без потерь, с высокой скоростью и на огромные расстояния, компактность источников и носителей информации, мгновенная реакция (отклик) инфосферы на трудно идентифицируемое в отношении источников воздействие и др[[9]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn9) .

В становление информационного терроризма свой вклад внесли хакеры, которые определили основные объекты кибератак и стали передовым отрядом кибертеррористов. Самыми престижными и интересными объектами для хакеров являются компьютерные сети силовых ведомств (прежде всего Пентагона) и НАСА. В каждом новом поколении компьютерщиков находится свой охотник до реальных приключений, решивший поиграть не в виртуальную, а в реальную ядерную войну. Основоположником движения хакеров-разрушителей можно считать чикагца Герберта Зина, более известного под сетевым псевдонимом (ником) “Сумеречный ястреб”. В 1987 году, будучи 17-летним юношей, он совершил одно из самых опасных вторжений в компьютерные системы министерства обороны США. Был обнаружен лишь после того, как снял копии программного обеспечения, прорвавшись к файлам системы управления ракетами США и базы ВВС Robbins. Он стал первым взломщиком, попавшим под закон США о компьютерных правонарушениях. Был приговорен к 9 месяцам тюрьмы и штрафу в 10.000 долларов.

Следующий крупный налет на информационные системы Пентагона был совершен уже организованной группой. В ноябре 1989 года хакер Zod, которым оказался 17-летний школьник из Нью-Йорка, проник в банки данных ВВС США и разрушил их, чем поставил под угрозу всю систему управления ВВС и носителями ядерного оружия. Впоследствии выяснилось, что еще в 14 лет Zod организовал группу единомышленников из 13 человек, называвших себя Masters of Doom в клубе хакеров Doom.

В 1990 году группа австралийских хакеров проникла в информационную сеть НАСА, что привело к остановке работы всей системы на 24 часа. Датские хакеры проникли в военные системы США, в компьютерные сети Центра космических исследований имени Кеннеди, командования флотом США и Ливерморской национальной лаборатории имени Лоуренса.

Информация о том, что в сентябре 1997 года хакер, проникнув в компьютерные сети НАСА и перегрузив его коммуникационные системы, подверг угрозе жизни находящихся в космосе астронавтов, стала известна лишь спустя три года из отчета ВВС. Правда, НАСА тут же опровергло это сообщение. “В нашей системы связи с орбитальными станциями никогда не было серьезных остановок благодаря атакам компьютерных хакеров, - заявили в НАСА, - Наши линии связи чрезвычайно хорошо застрахованы от такого проникновения”.

В феврале 1998 года гражданин Израиля Эхуд Тенебаум, известный в хакерском мире под ником Analyzer, организовал успешное нападение на компьютеры министерства обороны США. Инцидент совпал по времени с очередным усилением напряженности в районе Персидского залива, поэтому руководство Пентагона было уверено, что имеет дело с попытками Ирака помешать развертыванию американских сил на Ближнем Востоке. Для борьбы с хакером потребовались срочные усилия ФБР, ЦРУ, Агентства национальной безопасности, специальных исследовательских подразделений ВВС США, НАСА, минюста и Агентства защиты информационных систем, которые провели специальную операцию под кодовым названием Solar Sunrise. Действия Analyzer были названы американскими военными специалистами “одними из самых организованных и систематизированных, с которыми им приходилось сталкиваться”[[10]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn10) .

В январе 2001 года группа хакеров, именующая себя Pentaguard, провела массовое ”обезличивание” (deface) WEB-сайтов ряда государственных и военных структур США, Великобритании и Австралии. Первые страницы взломанных сайтов были заменены текстами, рекламирующими спиртные напитки, или просто краткими сообщениями типа “The largest gov&mil mass defacement in the history of minkind” (Крупнейший в истории человечества массовый взлом военно-правительственных сайтов). Отслеживающая хакерскую активность служба Attrition.org называла данную серию взломов самой масштабной в истории. Кстати, до этого группа Pentaguard совершала ”обезличивание” правительственных сайтов Китая, Кувейта, Румынии, Грузии и Вьетнама, однако эти масштабные акции никакой угрозы для национальной безопасности не представляли.

Так же регулярно атакуются компьютеры, принадлежащие Федеральной службе безопасности Российской Федерации. Есть даже статистика попыток взлома: каждый день, без перерывов на обед и выходные официальный сайт силовиков пытаются взломать около 15 раз. Сотрудник Управления компьютерной и информационной безопасности ФСБ России Владимир Непомнящий даже определил своеобразную географию источников: примерно половина злоумышленников действует с территории России, остальные базируются в ближнем и дальнем зарубежье[[11]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn11) .

Уже эти первые атаки информационных террористов весьма ощутимы для социума. Согласно данным, распространенным в апреле 2000 г. в Вене на Х конгрессе по профилактике преступности, общий доход террористов от компьютерных преступлений составляет 500 млн. долл. в год. Ущерб от их деятельности достигает 3,5 млрд. долл. в год и увеличивается ежегодно на 35%. Средние убытки от одного акта информационного терроризма составляют сумму около 560 тыс. долларов.

Строго говоря, перечисленные примеры относятся только лишь к части явлений, характеризуемых как “информационный терроризм”. В чистом виде - это “кибертерроризм” - умышленная атака на компьютеры, компьютерные программы, компьютерные сети или обрабатываемую ими информацию, создающая опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий[[12]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn12) . “Кибертерроризм” является составной частью информационного терроризма и служит фундаментом для реализации намного более сложных и разрушительных атак непосредственно на восприятие и анализ информации. Анализируя особенности развития инфосферы, можно смело предположить, что в обозримом будущем произойдет некоторое смещение в динамике целей информационного терроризма. Сегодня основными целями являются:

· несанкционированный доступ к информационным ресурсам с последующим похищением или искажением;

· формирование и массовое распространение по информационным каналам объекта террористических атак или глобальным сетям дезинформации населения;

· воздействия на исходные данные, используемые при формировании оценок и намерений принимающих решения лиц и общественности.

Уже сейчас предпринимаются попытки расширить этот список. Самые разные акторы стремятся посредством информационных технологий манипулировать общественным сознанием и политической ориентацией социальных групп населения страны с целью создания политической напряженности и хаоса. Дестабилизация политических отношений между партиями, объединениями и движениями провоцирует конфликты, разжигает недоверие и подозрительность. Обострение политической борьбы может спровоцировать репрессии против оппозиции и даже гражданскую войну. Снижение уровня информационного обеспечения органов власти и управления, инспирация ошибочных управленческих решений, дезинформация населения о работе государственных органов, провоцирование социальных, политических, национальных и религиозных столкновений, инициирование забастовок, массовых беспорядков и других акций протеста – все это подрывает авторитет государства и наносит ущерб жизненно важным интересам в политической, экономической, оборонной и других сферах.

Так что это за явление - информационный терроризм? Специальный агент ФБР Марк Поллитт[[13]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn13) определяет его как “заранее спланированные, политически мотивированные атаки на информационные, компьютерные системы, программы и данные, которые выражаются в применении насилия по отношению к гражданским целям со стороны субнациональных групп или тайных агентов”. Существенно расширяет данное понимание профессор Российско-Американского Университета Анатолий Исаков: “Информационный терроризм осуществляется в области, охватывающей политические, философские, правовые, эстетические, религиозные и другие взгляды и идеи, то есть в духовной сфере, там, где ведется борьба идей. Информационный терроризм - это, прежде всего, форма негативного воздействия на личность, общество и государство всеми видами информации.”[[14]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn14) С учетом всего вышеизложенного, под информационным терроризмом можно понимать умышленное применение отдельными лицами, террористическими группами или организациями средств информационного насилия с целью разрушения единого информационного поля, нанесения больших экономических потерь стране, создания атмосферы истерии в социуме, навязывания определенной линии поведения в процессе принятия решений. Цель информационного терроризма - максимальное снижение уровня информационной защищенности объекта воздействия. Достигается это путем решения ряда задач, основной из которых является поражение объектов информационной среды с помощью применения средств информационного оружия или информационного насилия.

**§ 3. Масштаб угрозы**

Информационный терроризм как современное социально-политическое явление представляет серьезную угрозу безопасности и жизненно важным интересам как личности, так и общества и государства. Очевидно, что применение террористами новейших достижений науки и техники сильно расширяет их разрушительные возможности, позволяет привлекать к себе всеобщее внимание и держать людей в постоянном страхе. Высокотехнологичный терроризм новой эпохи способен продуцировать системный кризис всего мирового сообщества, особенно стран с развитой инфраструктурой информационного обмена.

По оценке американских экспертов, эффективность информационного терроризма может быть сравнима с применением оружия массового уничтожения. По их мнению, угроза осуществления информационного терроризма прямо пропорциональна уровню технологического развития и масштабам использования компьютерной техники в системах управления государством. А это сразу позволяет определить те страны, которые уже сейчас наиболее уязвимы к деятельности террористов. Это с одной стороны, а с другой – обратить внимание на то, что в будущем весьма вероятно перемещение войны с терроризмом именно в инфосферу.

В настоящее время для террористов легко уязвимы практически все компьютерные средства обработки и хранения информации. Банковские, биржевые, архивные, исследовательские, управленческие системы, Интернет, средства коммуникации от спутников до мобильных телефонов, электронные средства массовой информации, издательские комплексы, всевозможные базы персональных данных - все это может атаковаться при соответствующей квалификации террориста с одного единственного компьютера. Мировые тенденции таковы, что информационный терроризм будет нацелен на мировую экономику. Методы информационного терроризма ориентированы не на физическое уничтожение людей и ликвидацию материальных ценностей, не на разрушение важных стратегических и экономических объектов, а на широкомасштабное нарушение работы финансовых и коммуникационных сетей и систем, частичное разрушение экономической инфраструктуры и навязывание властным структурам своей воли. Деньги - капитал вчерашнего дня, информация - сегодняшнего и завтрашнего. Например, Швейцария может претендовать на финансовое господство, но информационное обслуживание 80% банков этой страны находится в США. Вследствие этого компьютер сегодня становится самым многообещающим орудием преступности. Деловые центры обработки коммерческой информации и, прежде всего, компьютеризированные банковские учреждения являются самой доступной и заманчивой целью для терроризма. Террористический информационный удар по крупному банку способен вызвать системный кризис всей финансовой системы любой развитой страны, так как лишает общество доверия к современным технологиям денежного рынка. Продуманная кампания дезинформации, сопровождающая такой террористический акт, способна спровоцировать системный кризис. Опасность информационного терроризма неизмеримо возрастает в условиях глобализации, когда средства телекоммуникаций приобретают исключительную роль. Тревожные перспективы для развития информационного терроризма появились в связи с взрывным развитием сети Интернет, массовым и быстрым переходом банков, финансовых и торговых компаний на компьютерные операции с использованием разветвленных по всему миру электронных сетей. В поле зрения террористов оказались секретная информация, аппаратура контроля над космическими аппаратами, ядерными электростанциями, военным комплексом. Успешная атака на такие компьютеры может заменить целую армию. Очевидно, что заинтересованные структуры ведут непрерывный поиск вариантов, появляются новые средства нападения, оружие кибертеррористов постоянно модифицируется в зависимости от средств защиты, применяемых пользователями компьютерных сетей.

Целостность современного мира как сообщества обеспечивается в основном за счет интенсивного информационного обмена. Приостановка глобальных информационных потоков даже на короткое время способно привести к не меньшему кризису, чем разрыв межгосударственных экономических отношений. По заявлениям некоторых иностранных экспертов, отключение компьютерных систем приведет к разорению 20% средних компаний и около 33% банков в течение нескольких часов, соответственно 48% и 50% потерпят крах в течение нескольких суток.

Интернет - это динамическая, в значительной степени самоорганизующаяся система, позволяющая говорить о новом социальном явлении - открытом Интернет-сообществе. Официальных данных о том, насколько мир охвачен Интернетом, не существует, однако степень его проникновения можно оценить косвенно - как это сделали в компании NUA[[15]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn15) . Согласно последним доступным данным число пользователей Интернета составляет более 600 миллионов человек. Третья часть из них приходится на США. По данным Организации Объединенных Наций (UN World Report), примерно 15% населения Земли производит практически все технологические инновации и строит планетарную коммуникационную инфраструктуру. Примерно 55% населения способны воспользоваться плодами этих технологий и инфраструктуры, модернизируя на их основе производство товаров и услуг, а также государственное управление. В России прошедший год был исключительно успешным для рынка информационных технологий. Его рост за этот период составил 25,4%, а объем достиг 12 млрд. долларов. Хотя, по данным IDC[[16]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn16) , в 2006 и 2007 г.г. темп роста несколько снизится, среднее значение этого показателя в ближайшие пять лет останется на уровне 19%, а к 2009 г. объем рынка удвоится.

С конца 80-х годов в США неоднократно проводились исследования по изучению уязвимости информационных систем (ИС) различного назначения с точки зрения информационной безопасности. По итогам 1999 года в США зафиксировано около 250000 случаев вторжения в ИС государственного назначения (кроме ИС военного назначения). Почти 160000 (65%) таких вторжений оказались успешными. Зафиксировано свыше 160000 вторжений в ИС Министерства обороны США. Количество вторжений в ИС государственного и военного назначения каждый год увеличивается, в среднем, в два раза. Возросло количество случаев намеренного внедрения компьютерных вирусов в ИС государственного и военного назначения: с 583 в 1995 году и 896 - в 1996 г, до 1200 - в 1999 году. Начиная с 1996 года, в США зафиксирована тенденция роста числа случаев несанкционированного доступа в компьютерные сети федеральных ведомств и увеличение финансовых потерь от этих вторжений. Ежегодные потери достигают 5 млрд. долларов. По информации ФБР среди методов шпионажа все большую роль играют информационные. Так, Федеральная разведслужба Германии успешно провела операцию под кодовым названием RAHAB, в ходе которой осуществлялось программное вторжение в различные базы данных и компьютерные системы в США, содержащие информацию по электронике, авиации, химии, оптике, компьютерам и средствам телекоммуникаций.

Согласно данным Агентства национальной безопасности, США сильнее других стран зависят от сетевой инфраструктуры: здесь сосредоточено более 40% вычислительных ресурсов мира (для сравнения: в России - менее 1%) и около 60% информационных ресурсов Интернет. В США количество взаимосвязанных локальных сетей превысило 2 млн. Ежегодные потери от промышленного шпионажа, в соответствии с отчетами ФБР, составляют от 24 до 100 млрд. долларов. По оценкам Отдела науки и техники при президенте США, ежегодный урон, наносимый американскому бизнесу иностранными компьютерными вторжениями, достигает 100 млрд. долл. Потери от несанкционированного доступа к информации, связанной с деятельностью финансовых структур США, составляют не менее 1 млрд. долл. в год. Суммарный ущерб от компьютерных преступлений в странах Западной Европы за 1996 год составил порядка 30 млрд. долларов. Наиболее часто используемый канал, по которому осуществляется несанкционированный доступ - это сеть Интернет (65% случаев). В США 90% всей информации, в том числе и важной военной, переда­ется по гражданским сетям связи и сетям связи общего пользования типа Интернет[[17]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn17) . По результатам тестирования установлено, что 2/3 коммерческих и государственных Интернет-узлов не защищены от вторжения хакеров.

Внешние атаки могут преследовать и более серьезные цели, чем пассивный сбор данных, - такие, как, например, выведение из строя главных компьютерных узлов. По мнению экспертов, чтобы парализовать жизненно важные точки созданной инфраструктуры, достаточно нанести удар всего по нескольким десяткам объектов. В начале 1990-x годов в докладе Центра стратегических и международных исследований США “Киберпреступность, кибертерроризм, кибервойна - как избежать электронного Ватерлоо” был сделан вывод, что США не готовы противостоять угрозе возможных информационных атак, когда компьютеры, средства связи и программное обеспечение выступают в роли “оружия массового сбоя”, при помощи которого террористы могут проникнуть в американские компьютерные системы и нарушить их работу. Результаты тестирования в 1995-1996 г.г. Министерством обороны США 8932 информационных систем военного назначения с применением общедоступных средств проникновения, показали, что в 7860 (88%) случаях попытки проникновения обнаружены не были.

В 1997 г. для проверки надежности компьютерных систем защиты правительство сформировало группу из 35 компьютерных специалистов, которая, используя программы, свободно распространяемые в Интернете, смогла проникнуть в компьютерную сеть энергосистемы США и “отключить” энергоснабжение в ряде американских регионов. Кроме того, как сообщается, была полностью “выведена из строя” система управления войсками США на Тихоокеанском театре военных действий.

Агентство информационных систем министерства обороны США в целях проверки провело 38 тысяч “атак” по собственным компьютерным сетям - только 4% персонала, отвечающего за них, поняли, что производится “атака”, и лишь каждый 150-й сообщил в вышестоящую инстанцию о “вторжении”. Как утверждается в докладе, представители дружественных США государств также проникали в базы данных американских корпораций и использовали секретную информацию, стоящую миллиарды долларов.

По некоторым оценкам, в США на протяжении суток фиксируется не менее одной-двух попыток проникновения в информационные сети только одного министерства обороны США. Поэтому научно-технический комитет Пентагона (Defense Science Board) создал рабочую группу по проблемам защиты от информационных атак. Работа группы позволила определить целый ряд первоочередных задач в сфере информационной безопасности, на реализацию которых с 1997 по 2000 г. было выделено свыше 3 млрд. долларов.

Готовясь к возможному отражению террористических атак в инфосфере, Соединенные Штаты и сами сегодня продолжают совершенствовать информационное оружие и способы его применения. Так, из 22 критических технологий стратегического уровня, определяемых на перспективу, 12 (больше половины) касаются непосредственно информатики. Если в 1995 году министерство обороны США использовало 800 тысяч компьютеров, то через пять лет оно более чем в 2,5 раза увеличило свой компьютерный парк. Сегодня министерство обороны США использует более 2,1 млн. компьютеров, 10 тысяч локальных сетей и более 100 сетей дальней связи. За последние 10 лет общая доля расходов США на развитие информационных технологий и совершенствование информационного оружия возросла в три раза и достигла 20% военного бюджета[[18]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn18) . Затраты, запланированные США на реализацию концепции отражения атак в информационной сфере, до 2005 г. составят около 18 млрд. долларов.

Сказанное свидетельствует о том, что:

1. Сейчас, как никогда актуальна проблема информационного вторжения в компьютерные сети с применением информационного оружия. Выход этой угрозы на первый план связан с тем, что современные системы управления являются системами процессов критической значимости с высоким уровнем компьютеризации. Они могут оказаться весьма уязвимыми для внешнего воздействия, как в военное, так и в мирное время. Такое воздействие может привести к тому, что оружие сдерживания страны, подвергшейся агрессии, окажется полностью или частично заблокированным.

2. Широта спектра проявлений информационного терроризма, форм и способов его реализации, масштабы наносимого и потенциального ущерба породили сложнейшие задачи информационной защиты государства и общества.

3. Иностранные специалисты намного раньше отечественных поняли и оценили значение информационной безопасности, что послужило поводом к разработке стратегической концепции строительства вооруженных сил, в основу которой положено информационное превосходство над противником на всех стадиях развития конфликта. Американские военные считают, что это преимущество должно упрочить мировое лидерство США в 21 веке. Все это подтверждается докладами и дискуссиями на ряде международных конференций посвященных вызовам информационной эпохи, большую часть участников которых составляют сотрудники государственных учреждений, армии и разведывательного сообщества США - АНБ, ЦРУ, ФБР.

Глава 2. Информационный терроризм: технологии воздействия

**§ 1. Информационные технологии как инструмент влияния**

В настоящее время количество террористических актов неуклонно возрастает. Сложилось уже устойчивое понимание того, что современный терроризм не имеет единого источника, не является каким-то искусственным образованием или порождением злой воли какой-то социальной группы. Он - объективная, имманентная черта современного общественно-политического устройства мира. Современный терроризм - это уже устоявшаяся ситуация (политическая и социальная, психологическая и даже технологическая), наложенная на определенные идеологемы; это одна из ипостасей духа нашего времени в форме особой разновидности насилия. Как точка пересечения ситуаций и идей, информационный терроризм стал главным фактором современной политической и общественной жизни. Используя теоретические и практические достижения технического прогресса террор превратился в глобальную структуру и фактор, ведущий страшную разрушительную борьбу со всем цивилизованным миром. В наше время террористы приближаются к возможности угрожать безопасности всех стран и их граждан. Терроризм уже нельзя называть преступностью. Это уже настоящая война, можно даже сказать, что мировая. Одной из важнейших ее особеностей следует считать принимающую все большую значимость информационную составляющую.

На вопрос, что же делает информационные технологии столь перспективным инструментом влияния, впервые попыталась дать структурированный ответ РЭНД-корпорация[[19]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn19) .

1) Низкая стоимость входа: В отличие от ситуации с разработкой традиционных видов оружия, развитие информационных технологий не требует значительных финансовых ресурсов или государственного уровня финансирования. Достаточно иметь доступ к важным сетям и информационным системам. Нападение может осуществляться не только государствами, но также и негосударственными организациями, включая террористические группы и даже отдельных людей. Потенциальные противники могут обладать широким диапазоном возможностей, поэтому угроза национальным интересам существенно возрастает и постоянно видоизменяется. Многие специалисты полагают, уровень безопасности может быть поднят путем запрещения свободного доступа к сетям и системам управления, а также через эксплуатацию новых методов шифрования программного обеспечения. Подобные решения действительно могут снизить риск некоторых угроз, но важно подчеркнуть, что этот подход не исключает угрозу системе от предательства посвященных лиц (оператор систем) или от прямого физического нападения. Это также увеличивает трудности стратегической и тактической защиты.

2) Стертые традиционные границы: Сегодня связанные с традиционными географическими границами проблемы усложняются растущим взаимодействием в пределах информационной инфраструктуры. Учитывая множество возможных противников, оружия и стратегий становится все труднее различать иностранные и внутренние источники информационных угроз. Практически никогда нельзя точно знать, кто стоит за конкретным нападением или кто за него отвечает. Это сильно усложняет традиционное понимание правомерности с одной стороны, и национальной безопасности с другой. Еще одно следствие этого явления - исчезновение ясных различий между разными уровнями антигосударственной деятельности, в пределах от преступления до войны. Оппозиционно настроенные государства могут воздерживаться от традиционных типов военного или террористического противостояния и вместо этого эксплуатировать отдельных людей или межнациональные преступные организации с целью проведения ”стратегических преступных действий.”

3) Расширенная роль управления восприятием: Новые методики на основе информационных технологий позволяют существенно увеличить возможности для обмана и манипуляции восприятием, что значительно усложняет проблемы национальной безопасности. Возможности информационных технологий позволяют управлять потоками информации, являющейся основой общественного восприятия. Например, политические группы или неправительственные организации могут использовать Интернет и другие медиа-ресурсы, чтобы организовать политическую поддержку нерациональных решений. Возникает возможность прямого “создания фактов” и управления ситуацией методами информационного воздействия. И наоборот, внутренняя поддержка для спорных политических действий может быть легко уменьшена до несущественного уровня влияния. Очевидно, что прогрессивная государственная администрация должна включать информационный компонент в основу любой публичной кампании. Правительство должно заранее ”захватить контроль и управление” средствами массовой информации в ответ на вероятное информационно-стратегическое нападение. В ближайшем будущем органы государственной власти будут все чаще сталкиваться с задачей формирования и поддержания внутренней общественной солидарности в пользу любого планирующегося проекта.

4) Новый уровень стратегического анализа: Стратегические информационные уязвимости уменьшают эффективность классических способов сбора и анализа информации. Должна быть разработана новая область анализа, сосредоточенного на стратегической информационной парадигме, а традиционный набор средств может иметь лишь ограниченное применение в данной области. Важной проблемой является трудность выделения и распределения целевых финансовых и информационных ресурсов, т.к. государство может иметь трудности даже в опознании потенциала вероятных противников, их намерений, их возможностей, да и в идентификации самих противников тоже больше вопросов, чем ответов. Это означает необходимость построения новых организационных отношений внутри разведывательных сообществ, а также между этими сообществами и другими акторами. В контексте выбора между разведывательной необходимостью и соблюдением законности в гражданской сфере защиты информации следует опираться на нужды национальной безопасности.

5) Невозможность создания системы тактического предупреждения и оценки нападения: В настоящее время не существует адекватной системы предупреждения нападения, которая была бы способна отличить стратегические информационные нападения, а также другие виды информационно-террористических действий, включая шпионаж, от обычных несчастных случаев, отказов систем и сбоев программ. Государство никогда не может точно знать, происходит ли атака, как и кем она осуществляется.

6) Трудность создания и поддержки коалиций: Невозможность осуществления единого контроля за коммуникационной инфраструктурой всех партнеров коалиции, а также разный технологический уровень обеспечения устойчивости к стратегическому информационному нападению дает вероятным противникам непропорциональное преимущество. Каждая в отдельности страна коалиции будет по-своему уязвима к информационным нападениям на ее ключевые коммуникации. Например, развитие сотовых телефонных сетей ставит в зависимость страны с хорошо защищенными коммуникациями от тех, чьи сети легко доступны для преступных и враждебных проникновений. Другие сектора, особенно на ранних стадиях эксплуатации и в развивающихся странах, например, энергетика или финансы также находятся в группе повышенного риска. И наоборот, будущие партнеры по коалиции, особенно те, кто срочно нуждается в военной помощи, могут требовать гарантий того, что развертываемые в их регионе иностранные системы имеют должную защиту. В настоящее время существуют только общие проекты соглашений между возможными участниками, обозначающие защитные системы и концепции взаимодействия, но никакой определенной политики не разработано и даже не предложено в обсуждениях.

Сегодня, информационные системы настолько критичны к военным действиям, что часто более эффективно напасть на информационные системы противника, чем концентрироваться на разрушении его военных сил непосредственно. Также, современные общества сами по себе так зависят от информационных систем, что часто наиболее эффективный способ нападения на противника состоит в том, чтобы напасть на его гражданские информационные и коммерческие коммуникации, радиовещательные сети, финансовые системы данных, системы управления транспортом, и так далее. Мало того, что эта стратегия более эффективна в нанесении вреда противнику, она часто сама по себе имеет особые преимущества[[20]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn20) .

Вот лишь некоторые из потенциальных источников угрозы, применительно в частности к США[[21]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn21) :

· Коммуникации. Приблизительно 95 процентов всех военных коммуникаций в США осуществляются через коммерческие линии. Это ставит Американские вооруженные силы в неприятную зависимость от надежности и конфиденциальности этих коммуникаций, поскольку в некоторых случаях даже высоко секретные данные передаются в зашифрованной форме через коммерческие сети. И хотя другие страны не имеют возможности перехватывать и расшифровывать сигналы, они могут попытаться атаковать незащищенные должным образом коммуникационные инфраструктуры, нарушая тем самым работу военных систем связи или создавая бесполезные многочисленные информационные потоки, засоряющие и перегружающие каналы и обходящиеся в сотни миллионов долларов.

· Электроника. США закупают большинство микросхем, используемых в военных системах, у коммерческих производителей, многие из которых расположены в других странах. Эти микросхемы применяются в различных видах вооружений и исполняют обширный диапазон функций. Некоторые эксперты обеспокоены тем, что существует потенциальная возможность несанкционированного вмешательства в производство этих микросхем с целью внедрения посторонних элементов, выводящих систему из строя по сигналу извне.

· Асимметричный ответ. Малые и средние государства, а также террористические организации не могут вступать в открытый военный конфликт с США и его союзниками, поэтому они могут прибегнуть к тактике асимметричных угроз, не опасаясь ответного возмездия. Например, послать несколько сотен многообещающих студентов в образовательные учреждения, чтобы они стали компьютерными экспертами. Впоследствии эти специалисты смогут как организовать обучение у себя на Родине, так и систематически атаковать американские правительственные и гражданские сети и системы. Получив государственный уровень поддержки, они будут иметь возможность максимизировать наносимый ущерб, а также поддерживать надлежащую секретность проводимых операций, не позволяющую идентифицировать источник нападения.

· Экономический фактор. Некоторые эксперты полагают, что “экономическая война” между странами - область реального международного противостояния. Это действительно так, и спецслужбы всегда тайно помогают промышленности своих стран конкурировать на международной арене. Например, фиктивный “beta-испытатель” может срывать выход нового программного обеспечения на рынок, утверждая на интернет-форумах, что предварительная версия программы имеет серьезные проблемы.

· Полная компьютеризация. Современные военные самолеты, типа B-2 или F-22, разработаны без единого бумажного чертежа. Авиакорпорации используют специальную информационно-производственную систему, в которой все рассчеты и производственные инструкции выполнены на электронных носителях и распределены в закрытой сети. Это позволяет радикально улучшить бизнес-процессы предприятий, заводы которых расположены по всей стране. Но это также делает их сильно завимыми от надежности и безопасности коммуникационных сетей, которые могут быть подорваны, в том числе, и лицами с секретным доступом. Помимо этого, Военные ведомства используют современные методы организации снабжения “точно-в-срок”. Чтобы сокращать затраты и улучшать эффективность, военные по минимуму составляют запасы и резервируют оборудование на складах, а для ведения всего учета используют компьютеры. Если компьютеры ломаются - все останавливается.

· Программное обеспечение. Фактически в каждой современной системе оружия, развернутой сегодня есть программное обеспечение. Если оно хотя бы частично искажено, даже самые лучшие системы становятся бесполезными.

Многие исследовательские центры в последнее время активно изучают различные угрозы национальной безопасности. В этой связи важно помнить, что, в дополнение к угрозе вооруженным силам, многие, и даже большинство угроз обращены к коммерческой промышленности и гражданской инфраструктуре. Фактически все системы коммуникаций управляются компьютерами, все самолеты, корабли и наземные транспортные средства имеют программные компоненты, таким образом, все эти гражданские системы являются потенциальными целями враждебных стран.

Итак, ключевыми особенностями информационного терроризма являются:

· сравнительно низкая стоимость создания различных видов информационного оружия, используемого при проведении терактов;

· крушение статуса традиционных государственных границ при подготовке и осуществлении терактов, что выводит войну с терроризмом в совершенно иную плоскость;

· усиление роли управления восприятием ситуации путем манипулирования информацией по ее описанию;

· усложнением проблем обнаружения подготовки и начала осуществления терактов.

По оценкам начальника штаба ВВС США, сегодня около 100 стран мира владеют информационным оружием, которым могут завладеть и террористы. Более того, если, говоря о возможностях использования террористами ядерного, биологического и химического оружия, важно отметить, что создание этих видов оружия собственно террористами все-таки проблематично, то в отношении информационного оружия данная тенденция работать не будет, т.к. в информационном обществе значительно возрастает роль индивида, который может использовать свои творческие способности как во благо, так и во зло для человечества. В докладе Объединенной комиссии по безопасности, созданной по распоряжению министра обороны США и директора ЦРУ в июне 1993 г. и завершившей свою работу в феврале 1994 г., говорилось: “уже признано, что сети передачи данных превращаются в поле битвы будущего. Информационное оружие, стратегию и тактику применения которого еще предстоит тщательно разработать, будет использоваться с ”электронными скоростями” при обороне и нападении...”[[22]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn22)

**§ 2. Средства информационного оружия**

Под информационным оружием следует понимать - совокупность средств, предназначенных для нарушения (копирования, искажения или уничтожения) информационных ресурсов на стадии их создания, обработки, распространения и хранения. Основными видами информационного оружия можно считать[[23]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn23) :

\* компьютерные ”вирусы” - специальные программы, которые внедряются в программное обеспечение компьютеров, уничтожают, искажают или дезорганизуют его функционирование. Они способны передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и т.п. Кроме того, ”вирусы” способны самостоятельно размножаться, то есть копировать себя на магнитных носителях. Эксперты службы компьютерной безопасности США 24 сентября 2001 года заявили об обнаружении нового компьютерного вируса, связанного с ”кровавым вторником” (11 сентября). Вирус под названием “Военный глас” распространялся по электронной почте в виде письма с заголовком “Мир между Америкой и исламом” с вложенным в него файлом WTC.exe. В тексте письма содержалось обращение на английском языке: ”Привет. Не наступила ли война между Америкой и исламом?! Давайте проголосуем, чтобы жить в мире!” При попытке открыть приложение вирус начинал уничтожать все файлы на жестком диске, заменяя их новым текстом: ”Америка! Несколько дней покажут тебе, что мы можем сделать! Пришла наша очередь. ZaCker'y, тебя очень жалко”. Затем ”Глас” переходил к удалению антивирусного программного обеспечения, параллельно рассылая зараженную почту по всем записям адресной книги;

\* “логические бомбы” - программные закладные устройства, которые заранее внедряют в информационно-управляющие центры инфраструктуры, чтобы по сигналу или в установленное время привести их в действие. Отличие от компьютерных “вирусов” заключается в том, что существует разновидность “бомб”, которые вводятся в микропроцессоры или микросхемы памяти на уровне кристаллов и не могут быть обнаружены программными средствами. В определенное время или по внешнему сигналу такие “логические бомбы” переписываются на жесткий диск и начинают разрушение программного обеспечения компьютеров в сетях. Другая разновидность логических бомб – “прошитая” (интегрированная) в микросхемах программа, взламывающая защиту от несанкционированного доступа. Она дает возможность считывать информационные ресурсы без их видимого разрушения для добывания конфиденциальной информации. С помощью такой программы возможно целенаправленное изменение информации, которой пользуется потребитель, с целью его дезинформации. Как пишет американская печать, ЦРУ разработало и начало осуществлять мероприятия, согласно которым все микросхемы, которые могут быть использованы в военной технике других стран и поставляемые из США и других западных стран, должны хранить в своей памяти “логические бомбы”. Система получила название “chi ping”. Ярким свидетельством применения данного вида информационною оружия является опыт войны в Персидском заливе: Ирак не смог применить против многонациональных сил закупленные во Франции системы ПВО потому, что их программное обеспечение содержало логические бомбы, которые были активизированы с началом боевых действий[[24]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn24) ;

\* программные продукты типа “троянский конь” - программы, внедрение которых позволяет осуществлять скрытый несанкционированный доступ к информационному массиву объекта террористической атаки для добывания интересующих данных;

\* нейтрализаторы тестовых программ, обеспечивающие сохранение естественных и искусственных недостатков программного обеспечения;

\* преднамеренно созданные, скрытые от обычного пользователя интерфейсы для входа в систему. Они, как правило, сознательно вводятся в программное обеспечение программистами-разработчиками с далеко идущими целями;

\* малогабаритные устройства, способные генерировать электромагнитный импульс высокой мощности, обеспечивающий вывод из строя радиоэлектронной аппаратуры, а также другие средства подавления информационного обмена в телекоммуникационных сетях, фальсификации информации в каналах управления;

\* различного рода ошибки, сознательно вводимые в программное обеспечение объекта.

Один из видов оружия, который также может быть отнесен к информационному, - это средства радиоэлектронной борьбы. Они включают в себя средства радиоэлектронного подавления, радиоэлектронной защиты и радиоэлектронного обеспечения. Радиоэлектронная борьба в больших масштабах началась во время воздушной войны между Германией и Великобританией осенью 1940 года, получившей название “Битва за Англию”. Англичане с высокой эффективностью использовали постановку ложных радиомаяков и создание помех радиообмену. Таким образом, более половины немецких самолетов были дезориентированы и не достигали объектов бомбометания. Оторвавшиеся от своих самолетов прикрытия немецкие бомбардировщики становились легкой добычей английских истребителей. Известны случаи, когда по ложным радиомаякам немецкие летчики направляли свои самолеты на английские аэродромы в полной увереииости, что вернулись на свои базы.

Дальнейшая разработка этого оружия продолжалась с использованием спутников. Практическое опробирование в больших масштабах на поле боя было произведено в шестидневной войне на Ближнем Востоке в 1967 году и во время конфликта Великобритании и Аргентины из-за Фолклендских (Мальвинских) островов в 1982 году. В обоих случаях с американских спутников подавлялись частоты, на которых велась радиосвязь, и накладывались помехи на отраженные сигналы радиолокаторов. Во время обострения отношений США с Ливией и столкновений ливийских и американских истребителей в заливе Большой Сирт были использованы системы постановки помех и ложных радиомаяков. В результате было сбито 10 ливийских истребителей, а американцы не потеряли ни одного.

Теперь у средств радиоэлектронной борьбы появился новый объект - компьютерные сети и сами компьютеры. Задача осталась прежней - постановка помех и подавление информационного обмена. Ситуация усложняется с внедрением оптоволоконных кабелей, по которым циркулируют не потоки электронов, а световые импульсы. Однако известно, что уже созданы мощные генераторы электромагнитного излучения, имеющие преобразователи электрических сигналов в световые. Испытания проходят системы разрушения оптоволоконных кабелей с помощью лазеров[[25]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn25) .

Каждая страна, организация, в том числе и террористическая, может делать акцент на том или ином виде информационного оружия, на той или иной его компоновке. Например, в директиве Комитета начальников штабов США ”Борьба с системами управления” в качестве основных компонентов информационного оружия в сухопутных войсках США выделяют: интегрированную систему радио- и радиотехнической разведки и радиоэлектронного подавления (Intelligence and Electronic Warfare Common Sensor); систему комплексной высокоточной радио- и радиотехнической разведки (Guardrail/Common Sensor); систему армейской многофункционаяышй авиационной разведки ARL-M (Airborne Reconnaissance Low - Multifunction); систему воздушной разведки и целеуказания на базе тактического беспилотного летательного аппарата ”Аутрайдер” (Outrider Tactical Unmanned Aerial Vehicle).

Универсальность, скрытность, многовариантность форм программно-аппаратной реализации, радикальность воздействия, достаточный выбор времени и места применения, наконец, экономичность, делают информационное оружие чрезвычайно опасным: оно легко маскируется под средства защиты, скажем, интеллектуальной собственности, но позволяет при этом очень эффективно проводить акты информационного терроризма.

В качестве отдельного вида информационного оружия следует выделить Средства Массовой Информации, в особенности Телевидение и Интернет.

Современное телевидение предоставляет широкие возможности получать текущую событийную информацию. Оно в значительной мере организует досуг, отдых, развлечение. Время, проведенное у телевизора, за последние годы выросло и составляет значительную часть временного бюджета человека, семьи. Так, по данным зарубежных социологов, средний англичанин проводит у телевизора 12 лет из 70-летней жизни; в США средняя семья посвящает телепередачам 6,2 часа в сутки; 95% японцев смотрят передачи телевидения ежедневно; 87,4% французов посвящают телевидению большую часть своего свободного времени. Секрет такой популярности заключается, в основном, в следующем:

во-первых, телепередачи наиболее просты для восприятия (книга, газета требуют некоторого минимума инициативно-волевого усилия);

во-вторых, они создают эффект личного присутствия при событии;

в-третьих, по мнению психологов, до 40% всей чувственной информации об окружающем мире, о себе человек получает с помощью зрения.

Зрительный ряд обычно не требует словесного или письменного описания. Информация, получаемая зрителем, носит в значительной мере целостный, образный характер, а потому и весьма доступна. Человек уже привык, сидя в удобном кресле дома, смотреть передачи с исторических по значению конференций, с борта Международной Космической Станции, с арен Олимпийских игр, из столиц далеких государств. Телевидение как бы приблизило к человеку весь мир, сделало его доступным. Однако эта возможность информирования масс часто используется сугубо в политических интересах и выступает как один из ведущих инструментов манипулирования сознанием масс. Приемы этого манипулирования довольно просты, но достаточно эффективны:

\* Значительная часть телепередач носит развлекательный характер и в основном рассчитана на эмоциональное восприятие[[26]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn26) . Поэтому режиссеры телетрансляций делают особый упор на манипулирование иллюзиями: возможности хорошо заработать, достичь неожиданного успеха. Это делается не только с помощью художественных лент, но и тщательно подобранной документалистики. При помощи этой “машины грез” иллюзии занимают важное место в мышлении человека, создают эфемерное представление об обществе, в котором живет зритель: обществе якобы “равных возможностей”, подлинно “свободном”, “правовом”, “открытом” и “безопасном”. Разочарованные, часто обездоленные люди хватаются за призрачную идею “скрытых возможностей” общества, которое не исчерпало якобы своих потенциальных ресурсов. Некоторые телеканалы проводят линию по формированию специальной псевдокультуры, рассчитанной на оглупление масс, на притупление их общественного сознания.

\* Другой телевизионный прием манипулирования связан с эффектом дискуссионности различных точек зрения. При помощи этого приема создается видимость беспристрастности, объективности информации. Отрепетированная дискуссия или даже острая словесная перепалка, как правило по ничтожному вопросу, создают видимость борьбы мнений, сопоставления позиций и т.д., цель которых доказать, что другие альтернативные варианты по крайней мере не лучше навязываемого решения, а посему это “лучшее из других зол” следует одобрить и поддержать. В конечном счете пикировка лидеров движений, выступления общественных деятелей зачастую есть не что иное, как тщательно подготовленный политический спектакль, где сегодняшние слова ничего не значат для завтрашней практической деятельности.

\* Устойчивым телевизионным приемом является манипулирование словами-стереотипами. Например, популярные журналисты в своих программах широко манипулируют словами-образами, подкрепляемыми зрительным рядом: “международный терроризм”, “угроза демократии”, “тоталитаризм”, “фашизм”, “права человека” и т.д. Частое повторение этих выражений, сопровождаемое определенными видеообразами формирует заданное, и при этом весьма устойчивое представление в сознании слушателей. Поэтому во время политического комментария достаточно воспроизвести соответствующее выражение или наоборот - образ, как в сознании возникают вполне определенные характеризующие “главного врага” ассоциации.

Но все же в информационную эпоху все большую значимость приобретают мировые информационные сети, в частности Интернет, где можно создавать свои собственные сайты, отражать на них свое видение проблем, а также подбрасывать лживую информацию на чужие страницы[[27]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn27) . Существуют (по крайней мере, известны на сегодняшний день) не менее девяти возможных способов использования Интернета для содействия террористическим группам:

\* С помощью Интернета можно собирать подробную информацию о целях, включая изображение местонахождения целей и их характеристики. Если террорист получит подробную информацию о такой важной цели, как трубопровод или линия электропередач, он может манипулировать или шантажировать предприятия или правительство.

\* С помощью Интернета можно собирать деньги на поддержку какого-либо движения или играть на бирже, чтобы нажиться на разнице курсов акций после осуществления теракта. Некоторые сайты сепаратистов адресуют пользователей к банку и сообщают номер счета, на который можно послать деньги для их поддержки.

\* С помощью Интернета можно объединять людей. Теперь члены диаспоры, религиозной секты в любой стране или регионе мира, или сторонники любого движения (например, экологического), могут постоянно находиться в контакте. С помощью интернет-сайта можно давать указания о времени и месте встреч, формах протеста или вопросах для изучения.

\* Интернет можно использовать и для дискредитирования отдельных лиц, групп людей или компаний, например, финансовых институтов, а также для прямого лоббирования лиц, принимающих решения. Вымогатели требуют деньги у финансовых институтов с тем, чтобы последние избежали актов кибертерроризма и как следствие - ущерба своей репутации.

\* Интернет обладает огромным рекламным потенциалом и часто используется в этих целях. С помощью Интернета можно мгновенно обратиться как к массовой аудитории по всему миру, так и к отдельным лицам. Террористические группы ставят доступ к СМИ на первое место среди своих стратегических приоритетов. Террористы могут оставлять сообщения о будущих или уже спланированных действиях на страницах сайтов или рассылать их по электронной почте, а также брать ответственность за совершение того или иного теракта. Поскольку в информационную эпоху коммуникации - это власть, мировое общественное мнение стало приоритетом номер один.

\* Благодаря Интернету терроризм не ограничен лишь государством, где физически находятся террористы. Более того, в стране, подвергающейся теракту, баз террористов обычно вовсе нет.

\* Интернет может служить в качестве инициатора психологического террора. Часто психологическим аспектам Интернета не уделяют должного внимания. Благодаря кажущейся надежности Интернета, его можно использовать для того, чтобы посеять панику, ввести людей в заблуждение или обмануть. Интернет также стал благодатной почвой для распространения слухов.

\* Интернет существенно изменил коммуникационные сети террористов: в них теперь нет четких централизованных командных пунктов. Невольные соучастники террористов, например, хакеры, могут быть использованы “втемную” и не знать, для достижения какой цели их задействуют.

\* Интернет может быть использован и для отправки засекреченных сообщений, как ранее - симпатические чернила. Преступники могут обмениваться информацией по электронной почте и через электронные доски объявлений без опасения быть пойманными.

Террористы все чаще начинают использовать открытость цивилизованного мира для дискредитации правительств, подрыва доверия к ним населения, вывода из строя ключевых информационных систем, в том числе путем ввода в них определенных команд и вирусов. Во многих случаях это приводит к страху или панике граждан и таким образом дополняет традиционный терроризм. В прошлом было труднее организовывать и исполнять теракты из-за воздействия таких факторов, как расстояния и сложность координации действий. Сегодня Интернет - мощнейший инструмент информационного века - практически устранил обе эти проблемы. В результате появились новые, “сетевые” террористы, которые могут координировать свою деятельность на доктринальном, содержательном, организационном и социальном (лояльность) уровнях, используя новейшие технологические достижения[[28]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn28) . Об этом свидетельствует анализ ряда сайтов. Например, сайт “Кавказ-Центр”[[29]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn29) считается детищем “министра пропаганды Ичкерии” Мовлади Удугова. Главный сервер сайта находится в Калифорнии. На нем весьма оперативно появляется свежая информация о террористической деятельности на территории Чечни. Там же можно найти фоторепортажи о нападениях на федеральные войска, интервью с боевиками, отрывки видеозаписей терактов и другую информацию. Сайты “Чеченская Республика он-лайн”, “Правительство Чеченской Республики в изгнании” (сейчас не существуют в Российском Интернете) были рассчитаны на формирование положительного имиджа Чечни в глазах мирового сообщества. Здесь можно было узнать об истории Чечни, получить сведения о географическом положе­нии северокавказской республики, о ее богатых культурных традициях. На сайте “Информационного центра Ичкерия”[[30]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn30) , помимо традиционных фотографий, видеозаписей и интервью лидеров сепаратистов, присутствует подборка музыкальных файлов в формате mp3. Можно прослушать такие произведения, как “Гвардейцы Джохара”, “Шахид”, “Гимн Ингушского полка”. Многие другие сайты на самых разных языках содержат призывы к джихаду против “неверных”, здесь активно вербуются наемники для ведения боевых действий в Чечне, Афганистане и Индонезии, публикуются “инструкции по подготовке к джихаду у себя на родине”.

Электронная почта также сегодня активно используется террористами[[31]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn31) . Она позволяет экстремистам общаться в реальном времени, обмениваться текстами, фотографиями, видеоматериалами, сохраняя полнейшую анонимность. Соблюдение некоторых базовых мер безопасности делает обмен информацией практически недоступным для перехвата – даже с привлечением возможностей хорошо оснащенных спецслужб. Десятки поставщиков услуг электронной почты, такие, как Yahoo или Hotmail в США, Mail.ru в России позволяют, под ложным именем за несколько минут создать свой почтовый ящик и прекратить им пользоваться сразу же после получения или отправки первого послания. Не обязательно даже иметь свой компьютер и интернет-канал. Распространение во всем мире Интернет-кафе, включая развивающиеся страны, делает контроль за пользователями Интернет еще более проблематичным. В таких городах, как Бейрут или Гиза, уже есть десятки Интернет-кафе, а электронные послания можно принимать на сотовый телефон - как в Танзании, так и в Индонезии. Террористам не надо больше и встречаться лично: e-mail, чат, ICQ, IRC, форум - все это удобные анонимные способы обмениваться секретной информацией в реальном времени. При помощи видеокамеры сотового телефона можно делать многоминутные видеозаписи, в деталях отображающие маршрут, по которому необходимо следовать, чтобы не наткнуться на милицию, камеры видеонаблюдения, объекты атаки, - и тут же пересылать их исполнителям. Использование трехмерного изображения может помочь получить рельефный вид места будущего теракта или покушения для того, чтобы организовать отход отряда. Обзорные камеры, связанные с Интернетом, повторяющие построение сайтов типа Web-Cam, позволяют террористам вести непрерывное наблюдение за их целью без какого-либо вмешательства человека и из любой точки планеты, где есть выход в Сеть.

В настоящее время во многих странах ведутся разработки новых видов информационного оружия, которое бы непосредственно воздействовало на психику людей, управляло их поведением. По данным зарубежных источников, устойчивых и прогнозируемых способов руководства коллективным поведением людей пока не найдено. Однако в прессе периодически появляется информация об американской программе “МК-ультра”, а также аналогичных программах во Франции, Японии и других стран. Достижения в этой области таковы, что уже можно говорить об эффективности “зомбирования” (программирования поведения, деятельности) отдельных людей. Зомбирование достигается целым комплексом мер и средств. Среди них: химические (нейроэлептики, лекарства), обработка населения средствами массовой информации, психотронное оружие.

Под психотронным оружием понимаются средства воздействия на человека электромагнитными полями и волнами электронных приборов, вызывающее изменение его реакций на жизненные ситуации, возникающие в процессе жизнедеятельности. При этом происходят нарушение морфологического строения клеток и тканей организма. Некоторые средства массовой информации утверждают, что Россия в области создания психотронного оружия добилась серьезных результатов. “Московский комсомолец” в номере за 8 февраля 1995 г. даже опубликовал фотографии этого оружия. Комитет экологии жилища Российской Федерации также заявлял, что им известно о том, что в Советском Союзе была целая программа, созданная спецслужбами под руководством бывшего ЦК партии, названная операцией “Зомби”. Как считают представители данного комитета, эта программа предусматривала зомбирование или психотронную обработку большого количества людей. В печать просочились сообщения о том, что под Новосибирском была испытана установка, которая усыпила целую войсковую часть, и что к запуску в космос готовилась аппаратура, которая позволяла психотронным способом воздействовать на население, например, такого региона, как Краснодарский край[[32]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn32) .

Большой интерес в ряде стран проявляется к совершенствованию технических и других средств ведения информационных и психологических операций, таких, например, как топографические изображения в атмосфере, голосовые синтезаторы, позволяющие составлять провокационные сообщения и передавать их голосами лидеров различных государств или распространять посредством электронных СМИ. Зарубежные специалисты считают, что подобные средства физического и психического влияния на человека при 10%-й эффективности способны вызвать паническое состояние даже в хорошо организованном коллективе.

Таким образом, в структуре инфосферы можно выделить следующие основные объекты воздействия информационного оружия, которое может оказаться в руках террористов: программное и собственно информационное обеспечение; программно-аппаратные и телекоммуникационные средства; каналы связи, обеспечивающие циркуляцию информационных потоков и интеграцию систем управления; интеллект человека и массовое сознание.

Неожиданные по времени, месту, масштабам, способам, средствам действия или силе удары по информационной среде со стороны террористов, как правило, могут застигнуть объект воздействия врасплох, посеять панику, дезорганизовать управление, дестабилизировать обстановку и привести к серьезным последствиям. При этом всевозрастающие возможности информационного оружия предопределяют тенденции к внезапному осуществлению актов террора, длительному сохранению в тайне замыслов и планов предстоящих действий. Также следует отметить повышение скрытности подготовки применения сил и средств; искусную маскировку и дезинформацию. Террористы получают возможность наносить удары по информационной среде там, где никто не ожидает; примененять неизвестные объекту воздействия комбинации разных видов информационного оружия и способов решения задач. Однако цель по сути всегда одна – применить насилие для изменения ситуации в собственных интересах.

**§ 3. Информационное насилие**

“Насилие” – как ключевое понятие, характеризующее информационный терроризм – может проявляться в разных формах. В современных условиях намерение, направленное на нанесение ущерба субъектам действия или вещам, либо на уничтожение последних предполагает возможность не переходить к фазе уничтожения, а остановиться на фазе нанесения ущерба, причиненного путем создания атмосферы психологического давления на объект. Этот факт может весьма эффективно использоваться террористами. Именно информационное оружие, не являясь, по сути своей, средством физического насилия над личностью, способно “запускать” мощные вещественно-энергетические процессы и управлять ими во имя достижения конечной цели террористов. Сила влияния информации как раз и заключается в ее способности формировать и контролировать вещественно-энергетические потоки, параметры которых на много порядков превосходят разрушительный потенциал самой информации. Не являясь средством физического уничтожения, информация в то же время является средством насилия, которое может вести террористов к достижению поставленных целей.

Общество - это совокупность многих миллионов людей. Вся эта масса подразделяется на различные классы, объединения, группы, занимающие определенное место в социальной стратификации. И хотя каждому из таких подразделений, как и отдельным людям, свойственна своя система взглядов, подчас достаточно противоречивая, существует феномен общественного сознания, соединяющего людей в единое целое. Наше личное мнение может противоречить общественному, однако последнее не становится от этого сколько-нибудь менее реальным. Особой, определяющей чертой общественного мнения является его независимость от того, разделяет его или не разделяет каждый человек в отдельности. Ощутимая реальность общественного сознания состоит в том, что оно само, независимо от нашей воли навязывает нам свою реальность, вынуждая с собой считаться. Естественно, что жизнь человека, не разделяющего общественные воззрения, существенно отличается от жизни человека их принимающего. Общественное сознание - как и индивидуальное - в принципе должно адекватно отражать реальную обстановку, приспосабливаться к ее изменениям. Однако, сознание, как таковое, отделено от реальности и представляет самостоятельный объект, изменяющийся по своим законам. В частности, общественное сознание на каком-то этапе может носить иррациональный характер, подобно тому, как человек может жить в иллюзорном мире[[33]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn33) . В общественном сознании можно выделить три структурных уровня: верхний, основной и глубинный. К верхнему уровню можно отнести общественное мнение, которое носит изменчивый характер, относительно неустойчиво и имеет сравнительно малое время жизни. Основной уровень является аналогом картины мира у отдельного человека. О нем говорят как о парадигме. Этот термин характеризует установившуюся систему понятий, взглядов, мировоззрения общества в целом. Парадигма обладает большой устойчивостью. Глубинный уровень или подоснову общественного сознания можно грубо сравнить со слоями индивидуального сознания, формируемыми в раннем детстве и накладывающими свой отпечаток на всю жизнь. Тогда появляются символы и образы, лежащие в основе конкретного мышления человека. Данный уровень находит свое выражение в морали, идеалах, целях, ценностях, понятиях добра и зла, а также в духовных традициях народов. Он очень устойчив и при изменении парадигмы меняется незначительно. Более того, трансформация парадигмы происходит на базе имеющихся глубинных структур, которые, сохраняя основное содержание, приобретают новую форму.

Общественное сознание не статично, оно меняется. Сегодня огромная масса населения проживает в крупных городах - мегалополисах. Здесь сформировались особые условия проживания людей. Скученность, теснота, загрязнения, шум, интенсивное уличное движение, малоподвижный, но вместе с тем напряженный образ жизни, сокращение жизненного пространства порождают и обостряют различные виды заболеваний, в том числе аллергические и онкологические. В больших городах у многих людей возникают определенные психические сдвиги: неуравновешенность, агрессивность, подавленность, перманентное чувство одиночества. Неотъемлемыми чертами жизни становятся алкоголизм, наркомания, насилие, преступность. Растет маргинальная прослойка людей, которые не могут приспособиться к текущей действительности. В больших городах, где люди разобщены, очень высока степень их управляемости. Средства массовой информации, особенно телевидение, формируют моды, идеалы, нормы поведения. Неадекватно воспринимая окружающий мир, многие люди живут в мире абстракций и иллюзий. По существу же теряются традиции, преемственность поколений, связь времен и, как следствие, размываются фундаментальные маяки психической устойчивости, на которые ориентируется человек в своем поведении, поступках, решениях – что есть хорошо, а что плохо. Существующая тенденция позволяет говорить о глобальной неустойчивости общественного сознания. Атомизация общества оказала сильное негативное воздействие на его характеристики.

К настоящему времени изучен ряд неустойчивостей верхнего и основного уровней общественного сознания. Для верхнего уровня (общественного мнения) наблюдается маятниковая картина изменения векторов общественного сознания. Общественность, склонившись в пользу какой-либо из групп осуществления власти, при появлении серьезных трудностей начинает отклоняться в другую сторону, отрекаясь от бывших лидеров, и смещать центр тяжести своего влияния на процесс принятия решений в сторону альтернативных направлений развития[[34]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn34) . Например, за периодом диктатуры создаются условия для анархии, хаоса, безнаказанности и безответственности - как это было в 1990-е - после чего общество вновь стремится к жесткому порядку - как это происходит сейчас. В целом же колебания общественного мнения не приводят, как правило, к крупным потрясениям или катастрофам в обществе. Основной уровень (или парадигма общественного сознания) обладает значительной устойчивостью. Эволюция этого уровня может быть представлена как последовательная смена парадигм со скачкообразными переходами между ними. Эти переходы характеризуются на предварительной стадии крупномасштабными флуктуациями, неустойчивостями в мировоззрении отдельных групп и общностей. Процесс отхода от существующей парадигмы происходит на протяжении длительного времени, как правило скрытно. Например, как это было в СССР в начале восьмидесятых годов.

В этом контексте серьезной проблемой является применение различными акторами и структурами, в частности и террористическими, новых информационных методов воздействия на общественное сознание. Информационное насилие имеет существенные отличия от насилия традиционного, направленного на физическое подавление. Его суть - воздействие на общественное сознание таким образом, чтобы управлять людьми и заставить их действовать против своих интересов. Это можно рассматривать как определенный аналог вирусного заболевания. Так, вирус, внедрившийся в клетку, встраивается в управляющие процессами молекулы ДНК-РНК. Клетка внешне остается такой же, как и была, и даже процессы в ней идут такого же типа, но управляет ею вирус. Вирусное заболевание имеет скрытый латентный период, но после его окончания наступает острая стадия - организм переходит в возбужденное неустойчивое состояние. В этот период существенно повышается вероятность его гибели. Любая попытка изменить существующие порядки должна осуществляться в обстановке неустойчивости, только тогда она имеет реальные шансы на успех. И именно к этому стремятся террористы всех мастей – подвести общество к неустойчивости, дестабилизировать обстановку и “половить крупную рыбу в мутной воде”. Встраиваясь в процессы управления общественным сознанием, террористы зачастую не только не критикуют действия властей, но, напротив, стремятся выглядеть патриотами, выражать высшую преданность самым высоким ценностям. Среди применяющихся методов один из наиболее эффективных - постепенное доведение официальных государственных начинаний и лозунгов до абсурда, что компрометирует существующий режим в общественном сознании. В случае же появления каких-либо подозрений или обвинений всегда есть возможность оправдаться излишним, но похвальным усердием или, в худшем случае, глупостью. Характерным примером могут служить события в Чеченской республике РФ на протяжении 1990-2000-х годов, когда явные бандформирования “заботились” о традиционной культуре чеченского народа, “восстанавливали” мусульманскую духовность, “развивали” нефтяную промышленность[[35]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn35) . Любое общество неоднородно: существуют групповые интересы, национальные и региональные элиты, а также лица, стоящие у власти с их связями и интересами. Помимо внедрения своих людей в общественные и властные структуры, чеченские террористы активно продвигали дураков, карьеристов, обиженных властью, а также создавали условия для пропаганды тупиковых идейных течений и поддерживали их носителей. Одна из главных функций информационного насилия состоит в создании и раздувании противоречий. Это позволяет использовать многих людей “в темную”, когда они, решая собственные проблемы, борясь с конкурентами, фактически выполняют задачи злоумышленников. Существенно также, что террористы могут оставаться в глубокой тени и далеко не всегда выступать явными инициаторами тех или иных действий, а осуществлять операции на полутонах, максимально используя подставных лиц, борьбу тех или иных сил.

Ниже рассмотрены конкретные методы информационно-террористического воздействия на общественное сознание. Изложение строится на основе перехода от относительно простых методов к более сложным и изощренным.

Традиционно прямые рациональные способы воздействия на сознание основаны на убеждении людей, обращении к их разуму с применением рациональных аргументов, логики. При этом важно правильно понимать расстановку общественных сил, учитывать текущее состояние общественного сознания, реальные интересы людей, проводить научный анализ. Наряду с рациональными способами воздействия на сознание существуют способы, которые можно назвать иррациональными. Оказывая разрушительное воздействие, они подавляют рациональное начало и заставляют людей служить чуждым себе целям. Здесь можно выделить несколько методов:

Метод большой лжи. Считается, что восприимчивость масс довольно ограничена, их понимание - незначительно, зато забывчивость чрезмерно велика. В большую наглую ложь люди верят охотнее, чем в малую. Она дает выигрыш во времени, а потом о ней никто не вспомнит. На практике широко используются подлоги: полностью сфабрикованные или частично подделанные варианты реально существующих документов, материалов, свидетельств. А также слухи, представляющие собой искаженную информацию, не имеющую реального основания. Например, уже классическим приемом стало “изобличение бесчеловечных зверств режима” – в Косово, в Чечне, в Афганистане. Слухи рассчитаны преимущественно на людей с невысоким уровнем политического сознания. Распространяясь, слухи имеют тенденцию к гиперболизации, обрастанию фантастическими “подробностями”, “новыми” данными, “уточнениями”. Террористы всегда рассчитывают на то, что для широкого распространения конкретного слуха наиболее желательна обывательская, мещанская среда и наличие определенной эмоциональной почвы: возбуждения, неопределенности, ожидания каких-то событий. Неустойчивые люди, поддаваясь провокациям и разнося слухи, одновременно заражают общественность ложными представлениями и информацией.

В основе другого метода лежит ограниченность восприятия людей. Человек не успевает адекватно перерабатывать весь массив поступающих данных, его оперативная память ограничена, и избыточную информацию он воспринимает как шум. Поэтому действительно важную роль играют простые формулировки, повторение, закрепление определенного набора положений. Достаточно эффективными оказываются периодические, сменяющие друг друга (хотя бы и пустые) кампании, занимающие внимание людей, например, можно отметить периодически повторяющиеся кампании по борьбе с чем-либо: с коррупцией, с беззаконием, за права беженцев. Безрезультатность старых начинаний забывается, и все начинается снова. Шумная последовательность кампаний не оставляет времени для размышлений и оценок. Обеспечение информационной перегрузки в русле официальных взглядов, затрудняет возможность простому человеку разобраться в существе дела. В случае, если обман раскрывается, проходит уже какое-то время, острота вопроса спадает, а за этот период уже происходят определенные необратимые политические процессы, которые воспринимаются как нечто естественное, необходимое, вынужденное.

Третий метод основан на том, что в подсознании человека заложено определенное чувство принадлежности к определенной общественной группе, которое стимулирует моду, синхронизацию поступков, подчинение лидерам. На его основе террористы успешно пропагандируют свою исключительность “борцов за свободу и демократию”, солидарность со “свободной Европой”, выделенность из серой массы нецивилизованных “оккупированных” народов.

Нельзя не отметить и элементарный по сути, но глубокий по смыслу метод запугивания. Систематические нашептывания в эфире различных СМИ о нарастающих трудностях, неразрешимых противоречиях, апокалиптические прогнозы, мрачные комментарии порождают у слушателей, читателей, зрителей глубокий пессимизм, чувство обреченности и иррационального страха перед будущим. Такими людьми легче манипулировать, проще управлять, внушать определенные стереотипы политического мышления. Запуганный человек, поддаваясь воздействию “устрашающей” информации, психозу угнетающих фактов, становится беспомощным, индифферентным. Страх парализует не только волю, но и разум, чувства, понимание подлинной реальности.

Важно подчеркнуть, что методы информационного насилия особенно эффективны в нестационарных условиях, при быстро меняющихся событиях. Во всех случаях воздействия на сознание людей незримо присутствует фактор проверяемости. Недостоверная информация дает эффект только на определенное ограниченное время. В подсознании человека заложено сомнение, необходимость проверки, подкрепления информации. Поэтому при информационном воздействии в статических условиях посылка заведомо ложной информации невыгодна. Но весьма эффективен метод, часто используемый в рекламе: “Всегда говорите правду, говорите много правды, говорите гораздо больше правды, чем от вас ожидают, никогда не говорите всю правду”. Согласно этому методу, негативные стороны явления отождествляются с самим явлением. Негатив, каждый может, что называется пощупать, а само отождествление отодвигается в тень. Так, например, телевизионные репортажи о событиях, которые нужно представить в негативном свете, подаются с элементами документальности, но внимание зрителей сосредоточивается на кадрах, выхватывающих из большой толпы лица невменяемых людей, нелепые лозунги, хотя бы они и содержались в пропорции 1:100. При хорошей, профессиональной компоновке кадров можно создать для многомиллионной аудитории впечатление о событии, по сути противоположное реальности. Для любого подобного воздействия в существующих условиях все же необходимо присутствие правды и ее определенная дозированность, а уже этом фоне - необходимые порции ложных данных. Но эффективность воздействия заметно возрастает при более серьезной постановке вопроса - создании на основе истинных фактов ложной информационной структуры. Сложные образования такого типа носят название политических мифов[[36]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn36) .

Эффективное управление людьми, манипулирование ими с помощью информационного воздействия становятся возможными лишь при наличии обратной связи. В основе социологии массовых коммуникаций лежит схема: кто говорит, что сообщает, по какому каналу, кому и с каким эффектом[[37]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn37) . Последний момент имеет особую значимость. Вся схема информационного воздействия может работать вхолостую, если не принимать в расчет динамику сдвигов в сознании, а также возможностей неожиданности, непредсказуемости. В развитых странах происходит непрерывный зондаж общественного мнения. Существует целая система опросов, велика активность общения депутатов различных уровней с избирателями, большое внимание уделяется репрезентативности, точному выяснению умонастроений конкретных групп населения. Это позволяет вносить своевременные коррективы в процессы коммуникации, устранять возникающие рассогласования официальной идеологии и общественного сознания. Изучение опосредованного воздействия средств массовой информации, получившее название концепции многоступенчатого потока информации, показало, что параллельно каналам массовой и политической коммуникации, функционируют межличностные неформальные каналы информации[[38]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn38).

Основой ориентации человека служит складывающаяся в мозгу определенная “картина мира”, с которой сравниваются явления, наблюдаемые окружающей среде[[39]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn39) . Несоответствие ее реальности ведет к неадекватному поведению и с какой-то степенью вероятности к гибели. У человека и общества можно менять структуру мировоззрения с помощью внешних воздействий. Это осуществляется внедрением в сознание политических мифов, позволяющих заменить целостное мировоззрение фрагментарным. Совокупности мифов входят в мировоззрение современного человека и активно изменяют его объективную “картину мира”, приводя к неадекватному, искаженному пониманию реальности, своего рода психическим сдвигам. Крупнейший вклад в исследование мифов XX века внес немецкий философ Эрнст Кассирер. Его исследование, написанное более полувека назад, было связано с ситуацией в гитлеровской Германии. Но оно вполне корректно характеризует нашу действительность[[40]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn40) :

“Миф всегда трактовался как результат бессознательной деятельности и как продукт свободной игры воображения. Но здесь миф создается в соответствии с планом. Новые политические мифы не возникают спонтанно, они не являются диким плодом необузданного воображения. Напротив, они представляют собой искусственные творения, созданные умелыми и ловкими “мастерами”. Нашему XX веку - великой эпохе технической цивилизации - суждено было создать и новую технику мифа, поскольку мифы могут создаваться точно так же и в соответствии с теми же правилами, как и любое другое современное оружие, будь то пулеметы или самолеты. Это новый момент, имеющий принципиальное значение. Он изменил всю нашу социальную жизнь. Методы подавления и принуждения всегда использовались в политической жизни. Но в большинстве случаев эти методы ориентировались на материальные результаты. Даже наиболее суровые деспотические режимы удовлетворялись лишь навязыванием человеку определенных правил действия. Они не интересовались чувствами и мыслями людей. Современные политические мифы действуют совсем по-другому. Они не начинают с того, что санкционируют или запрещают какие-то действия. Они сначала изменяют людей, чтобы потом иметь возможность регулировать и контролировать их деяния. Обычные методы политического насилия не способны дать подобный эффект. Всегда остается сфера личной свободы, противостоящей такому давлению. Современные политические мифы разрушают подобные ценности. Наши современные политики прекрасно знают, что большими массами людей гораздо легче управлять силой воображения, нежели грубой физической силой. И они мастерски используют это знание. Политик стал чем-то вроде публичного предсказателя будущего. Пророчество стало неотъемлемым элементом в новой технике социального управления. Даются самые невероятные и несбыточные обещания, “золотой век” предсказывается вновь и вновь.”

В настоящее время, по сравнению с тем, что было 50 лет назад во времена Кассирера, благодаря взрывному развитию информационных технологий, процесс создания мифов резко ускорился. Теперь миф - это одна из центральных опор информационного насилия. Мифотворчество стремится так исказить сообщения о реальности, чтобы, несмотря на их неистинность, общественность принимала их как само собой разумеющееся и поступала бы в соответствии с этой деформированной информацией. В целом, это и есть механизм информационного насилия - манипуляция сознанием масс и внесение в общественное сознание целенаправленной дезинформации путем внушения людям соответствующих стереотипов мышления, выгодных заинтересованным акторам. При помощи информационного насилия можно менять жизненные установки людей в нужном направлении. При этом выделяется три уровня воздействия:

Первый уровень - усиление существующих в сознании людей нужных установок, идеалов, ценностей, норм. Закрепление этих элементов сознания в мировоззрении и жизненных установках.

Второй уровень связан с частными, малыми изменениями взглядов на то или иное событие, процесс, факт, что также оказывает воздействие на политическую позицию и эмоциональное отношение к конкретному явлению.

Третий уровень - коренное, кардинальное изменение жизненных установок на основе сообщения драматических, необычных новых данных, сведений.

Профессор Р. Гудин из Йельского университета (США) полагает, что с помощью манипулирования можно добиться изменения жизненных установок на первых двух уровнях воздействия. Кардинальные изменения взглядов человека, группы, общности требуют, по его мнению, комплексных воздействий на сознание в течение длительного времени[[41]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn41) .

В современной действительности манипулирование выступает как неотъемлемый атрибут образа жизни и управления мыслями и поступками людей. Образы и стереотипы общественного сознания вызывают соответствующее поведение, поступки, реакцию людей. Объективно, население конкретной страны почти не знает правды о событиях в соседних городах, регионах, и тем более странах. Ежедневно оно получает огромные порции информации, качество которой принимается на веру. Этим активно пользуются международные террористы: они приглашают журналистов, дают интервью, снимают фильмы. В общем, производят огромные массивы дезинформации, призванной убедить обывателя в “агрессивности”, “антидемократичности”, “бесчеловечности” официальных властей. При этом лишь одно упоминание стереотипа рождает в сознании человека привычные образы демонического, негативного, непривлекательного, и он как бы против своей воли верит в мифы и штампы террористической пропаганды. Постоянное оперирование соответствующими понятиями заставляет людей полагаться на предлагаемую интерпретацию событий, даже если внутренне они чувствуют, что их обманывают[[42]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn42). А полагаться на то, что сообщают независимые СМИ, общество зачастую вынуждено потому, что иная информации скудна или недоступна. Специалисты отмечают также, что одновременное распространение противоречивых взаимоисключающих суждений затрудняет адекватную ориентацию, порождает безразличие и апатию, провоцирует некритичность, возникает социальная дезориентация: большее впечатление производит не аргументированный анализ, а энергичное, уверенное, пусть и бездоказательное, утверждение. При помощи таких приемов террористы, а также различные некоммерческие организации, например, религиозные секты и различные фонды, пытаются манипулировать, а фактически управлять состоянием общественного сознания населения.

Манипулирование как важный элемент механизма информационного насилия реализуется посредством описанных выше методов и тесно связано с систематической дезинформацией населения, общества, определенных групп людей. Дезинформация есть не что иное, как сообщение, версия, имеющие целью сознательно ввести людей в заблуждение, навязать им превратное, искаженное или просто лживое представление о реальной действительности. Дезинформация подается с помощью различных форм: сенсаций, новостей, мнений. Чтобы поддерживать постоянный интерес общественности к наболевшему вопросу как у себя в стране, так и за рубежом, заинтересованные структуры эпизодически подбрасывают сенсации-сообщения, которые вызывают всеобщий интерес необычностью факта, явления или процесса. Понятно, что чаще всего сенсации “организуются”[[43]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn43) .

Обыватель мыслит стереотипами, навязываемыми его сознанию едва ли не с пеленок. Зная устойчивость, консервативность стереотипного мышления, различные организации террористического толка назойливо пытаются внедрить в общественное сознание разрушительные установки. Рекламная подача стереотипизированной информации – составляют главное содержание информационного насилия[[44]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn44) . Просеивая, отбирая, фабрикуя, урезая, искажая объективные исходные данные, информационный терроризм формирует извращенную картину социального бытия. Человек, общественные группы, массы людей, пользующиеся такой информацией, вольно или невольно смотрят на мир глазами террористов, вольно или невольно следуя их курсу, поддаваясь их обману. Находясь часто в мире оторванных от реальности символов, они могут идти даже против своих собственных интересов. Реальность может отходить на второй план, играть подчиненную роль. В этом смысле человек не является свободным, тем более, что давно отработан ряд способов эффективного информационного воздействия. Для них существует термин - “Brain washing” - промывание мозгов. С его помощью осуществляется зомбирование людей, создание пассивного послушного человека, превращение народа в легко управляемую массу. В этом плане понятия свободы, демократии, возможности волеизъявления на выборах должны быть подвергнуты серьезному переосмыслению[[45]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn45) . Любой деятель только тогда существует для масс, если он подается в СМИ. Теперь ни для кого не секрет, что с помощью средств массовой информации можно с невиданным мастерством создавать завесу обмана и иллюзии, так что становится чрезвычайно трудно отличить истину от лжи, реальность от подделки.

Манипулятивные возможности средств массовой коммуникации (СМК) достаточно хорошо известны исследователям, политикам, специалистам в области рекламы и имидж-мейкинга, заказчикам всевозможного рода рекламной продукции и т.д. Этим вопросам посвящены многочисленные исследования. Несмотря на некоторые разногласия в подходах к трактовке, различные авторы определяют три основные группы причин, обусловливающих манипулятивный характер СМК.

Во-первых, это причины, вызванные пристрастностью и субъективизмом людей, работающих в сфере массовой коммуникации. То есть, те искажения, которые вызываются их индивидуально-психологическими, личностными особенностями, политическими пристрастиями и симпатиями и т.п.

Во-вторых, это причины, вызванные политическими, социально-экономическими и организационными условиями, в которых осуществляют свою деятельность средства массовой коммуникации. Основная из них - зависимость СМК от конкретных социальных субъектов. Она может проявляться в двух основных формах - экономической и административной. Экономическая форма зависимости проявляется в том, что СМК в рыночных условиях работают на определенных клиентов, например, рекламодателей и других заказчиков из числа представителей крупного капитала. Административная форма зависимости проявляется в том, что СМК подчиняются своим хозяевам и учредителям.

В третьих, это причины, обусловленные самим процессом функционирования средств массовой информации. Для того, чтобы привлечь внимание и завоевать массовую аудиторию, СМИ при подаче материалов и подготовки сообщений, различных программ руководствуются определенными общими правилами или принципами. При этом, как отмечают В.П.Пугачев и А.И. Соловьев: “взятые ими на вооружение принципы отбора материалов плохо совместимы с глубокими аналитическими сообщениями и часто препятствуют созданию информационной картины мира, более или менее адекватной реальности”. Ими выделяется пять таких принципов[[46]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn46) :

1. Приоритетность (действительная и мнимая) и привлекательность темы для граждан. В соответствии с этим принципом наиболее часто сообщения СМИ касаются таких, например, проблем, как угроза миру и безопасности граждан, терроризм, экологические и иные катастрофы и т.п.

2. Неординарность фактов. Это означает, что информация о других экстремальных событиях - голоде, войнах, необычайно жестоких преступлениях и т.д. - доминирует над освещением явлений будничной, повседневной жизни. Этим объясняется, в частности, склонность СМИ к информации негативного характера и сенсациям.

3. Новизна фактов. Привлечь внимание населения в большей степени способны сообщения, еще не получившие широкой известности. Это могут быть новейшие данные о результатах развития экономики или численности безработных, о полете к другим планетам, о новых политических партиях и их лидерах и т.д.

4. Успех. Согласно этому принципу, в передачи и статьи попадают сообщения об успехах политических лидеров, партий или целых государств. Особое внимание уделяется победителям на выборах или в рейтинговых опросах. Культ звезд в политике, искусстве, спорте - типичное явление для СМИ в рыночном обществе.

5. Высокий общественный статус. Чем выше статус источника информации, тем значительнее считается интервью или передача, поскольку предполагается, что их популярность при прочих равных условиях прямо пропорциональна общественному положению людей, сообщающих сведения. В силу действия этого правила наиболее легкий доступ к СМИ имеют лица, занимающие высшие места в политической, военной, церковной или других иерархиях: президенты, военноначальники, министры и т.д. Им посвящаются первые страницы газет и главные радио- и телепередачи.

СМК формируют “массового” человека нашего времени. В то же время они разобщают людей, вытесняют традиционные непосредственные контакты, заменяя их телевидением и компьютерами. Восприятие формируется не книжной, как раньше, а экранной культурой. На этом фоне отмечается снижение способности к концентрации. “Массовый” человек импульсивен, переменчив, способен лишь к относительно краткосрочным программам действия. Он часто предпочитает иллюзии действительности[[47]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn47) :

“Современное информационное общество представляет собой особый тип и социального структурирования, и власти. После индустриального капитализма, базирующегося на владении средствами производства, после финансового капитализма, опирающегося на власть денег, наступает этап некоего символического информатизационного капитализма, в котором власть основана и осуществляется через средства коммуникации, путем управления информационными потоками. Средства коммуникации, оперирующие, трансформирующие, дозирующие информацию, становятся главным инструментом влияния в современном обществе. Для повышения эффективности осуществления властных стратегий используются самые современные информационные технологии, которые помогают превратить публику в объект манипулирования. Массовый человек, упрощенный, усредненный, повышенно внушаемый, становится этим искомым объектом. Сознание массового человека оказывается насквозь структурировано немногими, но настойчиво внедряемыми в него утверждениями, которые, бесконечно транслируясь средствами информации, образуют некий невидимый каркас из управляющих мнений, установлений, ограничений, который определяет и регламентирует реакции, оценки, поведение публики.”

Сказанное выше относилось к прямым методам воздействия на сознание. Но существуют и косвенные методы, связанные с воздействиями на условия функционирования мозга, на регулятивные функции. Так, в мозгу осуществляется химическое регулирование на основе нейромедиаторов и нейропептидов, которое может быть нарушено с помощью наркотиков и алкоголя. На сознание людей также могут существенно влиять электромагнитные и акустические поля, особенно в диапазоне инфрачастот. Обращая их на людей, сосредоточенных на относительно малом пространстве, можно существенно изменять их поведение, приводить к неадекватным, аномальным решениям[[48]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn48) .

Ранее, на всем протяжении истории, главным источником подавления людей служили физические методы воздействия - от изощренных пыток до современных средств массового уничтожения. Сейчас их с успехом заменило новое средство – информационное насилие.

**§ 4. Искусство “формировать реальность”**

Информационная среда – есть первостепенный источник формирования сознания человека, его самоидентификации, самостоятельности как личности, поэтому информационный терроризм есть война за контроль над разумом, а ведется такая война сетевыми методами.

Наилучшим образом сетевую атаку можно представить себе следующим образом: противником является не закованный в сталь супостат с мечом (гранатой, автоматом) в руке, а некая стая насекомых. Она тучей налетает сразу со всех сторон, проникая во все щели защиты, и кусает одновременно везде, куда может добраться. Каждое насекомое в отдельности не представляет никакой опасности, но атака целого их роя - это смерть. Вот это и есть сетевой терроризм. Основной его феномен американские специалисты РЭНД-корпорации Джон Аркуилла и Дэвид Ронфельдт видят в том, что раньше воспринималось как обычные партизанская война и мятежи, а теперь плавно переходит в форму социальной сетевой напряженности и становится глобальным террором - в пределе - мировой гражданской войной. Один из первых известных примеров такой социальной сетевой напряженности - это события в Сиэтле 1999 года[[49]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn49) , где совершенно неожиданно прошли массовые и чрезвычайно успешные выступления хитро организованных людей, которых для простоты назвали “антиглобалистами”, а из наиболее свежих – угрожающий рост количества различных религиозных сект, общественных движений, некоммерческих организаций, а также их влияния на общество.

По своей организации сетевой терроризм напоминает роение – именно этот термин упоминают в своих работах Аркуилла и Ронфельдт[[50]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn50) . Страна сталкивается с тем, что ее противник - какой-то рой вроде бы не связанных друг с другом фондов, комитетов в защиту того-то и того-то, преступных группировок, политических движений, телеканалов, интернет-сайтов. Только действуют они согласованно и в одном направлении. Здесь можно вспомнить, как России нанесли тяжелое поражение в Чеченской кампании 1995-1996 годов. Кто атаковал страну, добиваясь ее капитуляции перед сепаратизмом и бандитами? - Все те же роящиеся негосударственные структуры. Всякие партии, газеты, телеканалы, комитеты солдатских и других матерей, правозащитные группы и исследовательские фонды. Показательной является реакция многих СМИ и НКО на уничтожение лидера чеченских боевиков А. Масхадова российскими военными: это невосполнимая потеря на пути к миру в республике - теперь не с кем вести переговоры.

Основной метод ведения борьбы сепаратистов - навязывание многостороннего диалога между общинами метных жителей, международными наблюдателями и центральными властями. Для адекватного описания форм ведения сетевого террора уместно использовать термин “метадействие”, проявляемое во множественных ”микродействиях”, “тычках” и “стычках”: в выступлениях в СМИ, в вооруженных и невооруженных физических столкновениях, разного рода демонстрациях, презентациях, в навязываемых диалогах, оспариваемых выборах и пр. Для Аркуилла и Ронфельдта, и для самих сапатистов такого рода метадействия, безусловно, являются ни чем иным как войнами[[51]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn51) . Аркуилла и Ронфельдт, приводя многочисленные подтверждения из работ других исследователей, убедительно показывают, что такая социальная сетевая напряженность создается на транснациональной основе. Огромная роль здесь принадлежит правильному проектированию и использованию современных форм коммуникаций и информационных технологий, что, однако, не исключает, а, как правило, обязательно включает боевые отряды как небольшой по количеству, но важнейший элемент сетевых децентрализованных организаций, которые, собственно, и организуют эти метадействия[[52]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn52) .

Образ сетевого террориста получается каким-то неясным и рассредоточенным, его удары очень трудно отражать. Сама война, которую он ведет, превращается в тотальную, сплошную. Здесь нет фронтов, есть многомерное пространство войны, которая идет везде - в политике, культуре и экономике, в технологиях, на улицах городов и в идеологии. В этой войне в ход идут и убийства, и террористические акты, и вполне демократические дебаты, статьи в газетах и политические перевороты. И только иногда дело доходит до прямых традиционных террористических атак. Современный информационный терроризм похож на политический театр. Главной его целью является не убийство конкретных личностей, а воздействие на сознание широкого круга людей - устрашение и деморализация. Этим терроризм отличается от диверсионных действий, цель которых - разрушить объект (мост, электростанцию) или ликвидировать противника.

Аркуилла и Ронфельдт считают, что основой сетевой формы информационного терроризма сегодня становится бурно растущий третий социальный сектор. Это - огромное разнообразие самоуправляемых частных или неправительственных организаций. Именно эти организации и превращаются в тех самых роящихся насекомых, связанных почти неуловимыми командами в одну Сеть. Эти неправительственные организации не ставят перед собой задач распределения прибыли акционерам или директорам - они, помимо формального аппарата государства, преследуют общественные цели вовне. Все это начинает становиться “ассоциационной революцией” негосударственных действующих лиц, и по своему значению вполне может быть сопоставлено с возникновением национального государства в Новое Время[[53]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn53) . Как в свое время государства нынешнего типа с их бюрократией и центральной властью безжалостными хищниками ворвались в пестрый мир феодальной раздробленности, так и сегодня неправительственные организации, вездесущие и быстрые, врываются в мир неповоротливых государственных бюрократий. Разумеется, все прекрасно понимают, что такие негосударственные организации, выступают обоюдоострым оружием и используются для ведения сетевой информационной войны как отдельными небольшими террористическими организациями, так и самыми мощными государствами мира. Примечательная особенность характера сетевого терроризма является его гуманность, а в технологиях реализации – множественность. Здесь и политика, и экономика, и коммуникации, и социальная сфера одновременно являются объектами нападения.

Современная сетевая напряженность переводит реалии действительности в новое измерение – в “зазеркалье” сплошного террора, войны как процесса, как формы мира. Информационный терроризм будущего будет состоять из множества боевых процессов, одновременно происходящих “гроздьями”, “пучками”, многими “роями” по разным направлениям, содержаниям и составу участников. Время, пространство и террор совершенно сольются и превратятся в нечто, что предельно точно обозначил российский геополитик В.Л. Цымбурский как “непрерывность стратегического процесса”[[54]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn54) . На смену странной сетевой напряженности - многим непрерывным вооруженным и невооруженным конфликтам в мирное время - постепенно приходит сплошное насилие, в том числе, и в первую очередь, - информационное. Очень тонко чувствуют это лучшие российские профессионалы военного дела. Так, генерал-полковник запаса Л. Г. Ивашов, исключительно сильный военный дипломат, в своих статьях четко указывает на методологический принцип утверждения контрольно-управленческих функций над регионами и странами – “управление через хаос”. Также чутко и верно он определяет ситуацию как “близкую к мировой трагедии”, к так называемому феномену “мировой гражданской войны”[[55]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn55) . Конечно, хаос и “мировая гражданская война” - это весьма метафорические и неточные, построенные больше по аналогии, термины. Они отражают не понятия, необходимые для организации соответствующей обороны и армии, а общее название того, что происходит в виде “естественного” процесса - т. е. просто все понимают, что хаос, а откуда хаос и как этот хаос организован, уже почти никто не понимает и даже неспособен понять. Любой неверный шаг и методологическая слабость здесь обходится очень дорого. Можно указать только на один простой и наглядный пример:

Через несколько дней после 11 сентября 2001 года российское руководство поспешило отрапортовать о том, что у чеченских боевиков нашли компакт-диск с учебным пособием по вождению самолетов. Замысел был прозрачен до неприличия - заставить “мировое сообщество” признать чеченских боевиков международными террористами. Но признание Россией мирового терроризма как главнейшей проблемы чеченского кризиса, автоматически означает ее самозачисление в одну из двух категорий стран: в “мировую цивилизацию”, объявившую войну “международному терроризму и варварству”, или в “страны-изгои”, составившие “мировую ось зла”. Нахождение России в любой из этих категорий стран является и тактически, и тем более стратегически абсолютно тупиковым и чрезвычайно опасным. В одном случае Россия противопоставляет себя “арабскому миру”, что сразу же дает чеченским боевикам его неограниченную подддержку, а в другом – вынуждена идти на конфликт с Западом, отстаивая свое право на самостоятельное решение проблемы внутреннего очага напряженности. Никто даже не задумывается, а почему мы должны выбирать одну из навязанных альтернатив? - Мощные информационные потоки постоянно затачивают общественное мнение под нужным углом. И получается, что для обывателя все события происходят как-то сами по себе “в виде естественного и единственно правильного процесса”. Более того, имеется тенденция к отсутствию даже самой возможности выбирать.

Старые правовые, бюрократические государства становятся самой легкой мишенью для атак сетей и роев неправительственных организаций при информационной поддержке соответствующих СМИ. Они похожи на неуклюжие и медлительные клетки, атакуемые мелкими и чрезвычайно подвижными вирусами. Проходит немного времени - и вирусы захватывают клетку, подчиняют себе, заставляя ее саморазрушаться и плодить новые болезнетворные вирусы. Как написал еще в 1986 году теоретик малой войны Фридрих фон Хейдт[[56]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn56) “в неправильной иррегулярной войне правовое государство (конституционное республиканское государство в рамках западной традиции) имеет огромные проблемы... В правовом государстве мы имеем только два типа людей: законопослушные граждане и преступники. Третий тип людей, который ведет иррегулярную войну, правовым государством во внимание не принимается”. Концепции и идеологии правового государства попросту “не хватает” для того, чтобы адекватно выразить проблемы современного информационного терроризма: в классическом государстве все разделено по ведомствам. Одни чиновники борются с преступностью, вторые - налоги собирают, третьи - за культуру отвечают. Армия со внешними врагами должна сражаться. И так далее. И вот такое государство, в котором все виды деятельности разделены на ведомственные отсеки, подвергается нападению роя негосударственных структур. Они прорываются на стыках ведомственных интересов. То, что они делают, вроде бы находится на грани преступления, но за эту грань не заходит. Есть в их работе что-то подрывное - но все же это не террор в чистом виде. Есть в этих нападениях что-то от религиозного сектантства, от пропаганды, от экономической диверсии. Вроде бы деятельность негосударственных “роевиков” - ни первое, ни второе, ни третье, а общий эффект получается убийственным. И государство оказывается в тупике. Полицейские, пожимая плечами, норовят спихнуть дело на спецслужбы, а те - на налоговиков или на военных, а в результате никто ничем не занимается. Главное, на что указывает Фридрих фон Хендт и все те профессионалы, кто работает с феноменом терроризма или неправильных войн, - это то, что за любыми ”безличными” и “немотивированными” террористическими актами стоят совершенно конкретные лица и субъекты, страны и народы. Другое дело, что искать их, как правило, надо не там, где светло, а там, где они фактически есть.

Итак, подводя итог данной главе, следует подчеркнуть:

1. Мощность воздействия средств информационного оружия неизмеримо высока в соотношеннии с их доступностью для применения террористами.

2. Масштабы информационного насилия достигли критического уровня и вплотную подошли к границе, за которой уже невозможно отделить объективную реальность от субъективной.

3. Искусственно создаваемая перманентная общественная напряженность отрицательно влияет на прогрессивное развитие цивилизации, социума, каждого отдельного человека.

4. Современное государство должно форматировать свои взаимодействия со всеми контрагентами в контексте глубокого и многопланового анализа информационно-коммуникационных процессов.

**Глава 3. Противодействие информационным угрозам**

**§ 1. Минимально необходимые действия Правительства**

Один из способов лучше понять сущность информационного терроризма состоит в том, чтобы вспомнить развитие механизированных войн. Начиная с середины 19 века, Индустриальная Революция сделала возможным создать новые виды оружия, которые были гораздо более эффективны, чем что-нибудь произведенное прежде: массовое производство автоматов, паровые броненосцы, артиллерия дальнего действия и так далее. Военные также извлекли выгоду из технологий, которые были развиты, главным образом, для гражданских целей - железные дороги и телеграфы. Но которые значительно улучшили боеспособность вооруженных сил к мобилизации и маневренности на поле боя. Война стала быстрее, обширнее и более смертоносна. Но новые технологии также создали и новые цели. Военные силы стали критически зависимы от их национальной индустриальной основы - нет фабрик и заводов - нет массового производства оружия, что означает невозможность победы. Так разрушение национальной промышленности врага стало столь же важным как разрушение его армии, если не более.

Результатом послужили не только изменения в военном мышлении, но и полностью заново переработанные военные доктрины. Военные стратеги начали делать ставку на оружие дальнего диапазона, передние линии атаки перенеслись с поля битвы на фабрики врага, его железные дороги и телеграфные линии. Классический актуальный момент - прогресс от изобретения самолета к развитию полностью новой доктрины стратегической бомбардировки. Кроме того, предполагалось, что такой расширенный план войны стал не возможностью, а доминирующей стратегией.

Сегодняшняя информационная революция представляет собой подобную ситуацию. И также как новые теории и доктрины были развиты для войны индустриальной эпохи, так сейчас развиваются теории и доктрины войны информационной. Информационные системы настолько жизненно важны и военным, и гражданскому обществу, что они становятся главными целями в любом современном конфликте, и они могут также служить главными средствами для проведения наступательных операций. В действительности, информационное насилие - это темная сторона Века Информации. Уязвимость военных и общества есть прямой результат распространения информационных технологий. И наоборот, потенциал этих технологий как оружия - прямой результат технического прогресса[[57]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn57) . Действительно, многие из проблем связанных с информационным терроризмом коренятся в самой природе информационных технологий. Наиболее важная особенность - падение стоимости обработки информации: затраты 1950-ых снижались приблизительно на 90% каждые пять лет, и большинство экспертов ожидает, что эта тенденция продолжится в течение обозримого будущего. Информационные технологии, позволяющие организовывать информационный террор, постоянно становятся все более и более доступны. В отличие от ядерного или космического оружия, которые распространились устойчиво, но медленно, распространение информационных технологий, вероятно, ускорится. Если какая-либо страна не может позволить себе перспективные разработки сегодня, то она, вероятно, сможет позволить себе это завтра. Это доказано распространением военных электронных систем, но даже в большей степени применением коммерческой инфраструктуры типа компьютерных сетей, спутниковых и оптоволоконных коммуникаций, сотовых телефонных систем, и так далее. Все они могут использоваться для враждебных целей, и могут быть атакованы враждебными силами.

Вторая особенность информационной технологии, которая затрагивает информационную безопасность это то, что, поскольку технология становится все более дешевой, становится все труднее сохранять централизованное управление векторами развития. Действительно, увеличивающееся общественное давление ведет к децентрализованному управлению. Спрос и стимулы для децентрализации следуют за технологической возможностью. Дешевая информационная технология неизбежно ведет к потере контроля[[58]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn58) . Эта тенденция идет в противоречии с несколькими столетиями военных традиций и опыта, которые основаны на иерархических структурах командования и централизованном управлении. Новая технология не поддерживает традиционную военную модель. Также, тенденция к децентрализованным информационным системам меняет способность правительства взаимодействовать с коммерческим сектором. Как результат, должностные лица, ответственные за национальную безопасность и военные стратеги должны искать новые формы руководящих инструкций и новые способы осуществления контроля.

По этому вопросу хочется вновь обратиться к разработкам специалистов РЭНД-корпорации и изложить их рекомендации относительно политики государства, стоящего перед лицом опасностей информационного терроризма. Особенности и вероятные последствия стратегической сетевой атаки указывают на основной вывод: традиционные национальные военные стратегии являются устаревшими и неадекватны. Чтобы противостоять новой угрозе РЭНД-корпорация разработала пять главных рекомендаций[[59]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn59) :

1. Лидерство: Следует жестко определить конкретных руководителей государства, ответственных за информационно-коммуникационную сферу. В ответ на стратегическую информационную угрозу необходимо на уровне личного Президентского контроля сформировать соответствующую спецслужбу, поскольку только на этом уровне можно достичь необходимой координации большого количества правительственных организаций, вовлеченных в обеспечение национальной безопасности. Эта спецслужба должна отвечать за защиту всей национальной информационной инфраструктуры, включая коммерческий сектор. После формирования организационной структуры и обеспечения высшего уровня поддержки, она должна немедленно направить все имеющиеся ресурсы на управление всесторонним развитием национальной безопасности стратегических информационных коммуникаций и систем.

2. Оценка риска: Первым шагом в работе вышеописанной спецслужбы должна стать немедленная оценка рисков, с целью достоверно определить степень уязвимости ключевых элементов текущей концепции национальной безопасности и национальной военной стратегии. В этот обзор должны быть непосредственно включены стратегические прогнозно-целевые модели, описывающие возможные последствия предполагаемых сценариев развития событий. Без точной оценки риска в динамической информационной среде размываются основания для принятия стратегических президентских решений.

3. Роль Правительства: Изменение традиционной роли Правительства по отношению к национальной безопасности и интересами общественности заключается в организации более тесного взаимодействия со внутренним сектором экономики. В дополнение к повышению общей готовности противостоять информационным угрозам, необходимо усилить работу по переоснащению систем инфраструктуры, обучению персонала, проведению тренировок представителями спецслужб и военных. Правительство может значительно повлиять на предоставление налоговых и других льгот предприятиям, развивающим информационный сектор экономики. Хорошо организованная работа правительства в этой области должна быть сбалансирована и не должна приводить к потере гражданских свобод коммерческим сектором.

4. Стратегия национальной безопасности: Сразу после завершения начальной оценки риска следует заняться разработкой стратегии национальной информационной безопасности. Готовность государства к выявленным угрозам подразумевает работу по всем традиционным направлениям от “военных” до “гражданских”, от “иностранных” до “внутренних”, и от “национальных” до “местных”. Разумно было бы разработать и внедрить специальную Концепцию “минимальной обязательной информационной инфраструктуры” (МОИИ), которая была представлена как возможная стратегическая оборонная инициатива. МОИИ задумана как минимальная инфраструктура информационных систем, процедур, законов и налоговых стимулов, гарантирующих длительное функционирование государства даже в период сложной стратегической сетевой атаки. В качестве аспектов такой МОИИ могут быть представлены наборы правил и инструкций для Федерального правительства, поощрения владельцев и операторов различных национальных инфраструктур с целью уменьшить уязвимость их организаций и гарантировать быструю мобилизацию в момент информационного нападения. Аналогом может служить концепция стратегической ядерной Минимальной Обязательной Аварийной Сети (strategic nuclear Minimum Essential Emergency Communications Network). Многие специалисты считают МОИИ концептуально очень привлекательной даже при том, что существуют некоторые разногласия относительно того, как она должна быть организована. Оценка аспектов реализации МОИИ должна быть предпринята в как можно более ранние сроки.

5. Национальная военная стратегия: Национальная военная стратегия должна предполагать появление нового театра боевых действий – киберпространства. Слабость военного присутствия на географических пространствах может стать менее существенной угрозой, чем уязвимость в национальной информационной инфраструктуре. В этой ситуации есть риск, что страна может столкнуться с трудностями идентификации сетевого стратегического нападения. Президент всегда должен точно знать: подверглась ли нация атаке или нет.

Эти срочно принятые меры оставляют надежду, что вероятность наступления катастрофических последствий в результате вероятной агрессии будет значительно снижена, что оставляет хорошие шансы своевременно развивать и модернизировать эффективную обороноспособность в отношении перманентно растущей угрозы. Полностью обезопасить общество и государство от террористов невозможно, но можно снизить угрозу превентивным контролем за “интересными” для террористов местами и борьбой с непосредственными исполнителями террористических актов. Одна из задач состоит в том, чтобы сузить варианты действий террористов и контролировать те, что останутся. Например, правоохранительные органы России проводят работу по установке мониторинговых устройств в Интернете, с помощью которых можно просматривать сообщения, присылаемые по электронной почте, и отслеживать обращения пользователей к страничкам Интернета. Создаваемая система СОРМ (“Система оперативно-розыскных мероприятий”) предназначена в основном для выявления тех, кто уклоняется от уплаты налогов и других нарушителей, однако, по мнению противников ее внедрения, она будет равносильна всеобъемлющему нарушению конфиденциальности, что будет нарушать конституционные права законопослушных граждан. С другой стороны, есть предпосылки, что в ближайшее время преступления в сфере высоких технологий могут выйти на качественно новый уровень: нет необходимости захватывать самолет с заложниками, если намного проще угрожать жизни всех, кто находится в небе, через управляющий полетами компьютер. Небольшое изменение в программе - и результат достигнут.

Активные действия, предпринимаемые разработчиками средств защиты, пока не позволяют получить желаемой защищенности. В этих условиях организации не должны ограничиваться простым обновлением версий антивирусного ПО, брандмауэров и других приложений. Надежность корпоративных систем сегодня напрямую зависит как от применяемых технологий защиты, так и от наличия в организации комплексной стратегии в области информационной безопасности, а также от корпоративной дисциплины при ее практической реализации.

Становление информационного общества показывает, что нормальная жизнедеятельность общества и государства целиком определяется уровнем развития, качеством функционирования и безопасностью информационной среды. Производство и управление, оборона и связь, транспорт и энергетика, финансы, наука и образование, средства массовой информации - все зависит от интенсивности информационного обмена, полноты, своевременности, достоверности информации, которая может быть искажена с помощью средств информационного терроризма. Последствия таких актов могут быть весьма трагичными для социума. Поэтому задача отражения возможных атак со стороны террористов в инфосфере задает новые стандарты, выводит на принципиально иной уровень вопросы информационной безопасности.

**§ 2. Аспекты создания целостной системы информационной безопасности**

Считается, что для предотвращения или нейтрализации последствий применения информационного оружия со стороны террористов необходимо принять следующие меры: организовать защиту материальмо-технических объектов, составляющих физическую основу информационных ресурсов; обеспечить нормальное в бесперебойное функционирование баз данных; защитить информацию от несанкционированного доступа, искажения или уничтожения; сохранить качество информации (своевременность, точность, полноту и необходимую доступность); постоянно проводить работу по обеспечению высокого морально-психологического состояния населения страны, персонала инфосферы[[60]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn60) . Общие методы обеспечения информационной безопасности страны можно разделить на правовые, организационно-технические и финансово-экономические[[61]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn61):

К правовым методам обеспечения информационной безопасности относится разработка нормативно-правовых актов, регламентирующих отношения в информационной сфере, и методических документов по вопросам обеспечения информационной безопасности.

Отличительной чертой информационного терроризма является его дешевизна, сложность обнаружения и идентификации. Анонимность, обеспечиваемая Интернетом, позволяет террористу стать невидимым и, как следствие, практически неуязвимым и ничем (в первую очередь жизнью) не рискующим при проведении преступной акции. Положение усугубляется тем, что преступления в информационной сфере, в число которых входит и терроризм, влекут за собой наказание существенно меньшее, чем за осуществление “традиционных” террористических актов. В соответствии с Уголовным кодексом РФ (ст. 273), создание программ для ЭВМ или внесение изменений в существующие программы, которые заведомо приводят к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, наказывается лишением свободы на срок максимум до семи лет. Для сравнения, в США законы карают несанкционированное проникновение в компьютерные сети заключением сроком до 20 лет. Ведущие государства мира серьезно обеспокоены рассматриваемыми проблемами и это, как правило, быстро отражается в законодательствах этих стран.

В России также принят ряд документов, составляющих основу для дальнейшего совершенствования регулирования информационно-коммуникационных взаимодействий. Существует Доктрина информационной безопасности РФ от 28.09.2000, федеральные законы “Об электронной цифровой подписи” от 10.01.2002, “Об информации, информатизации и защите информации” от 20.02.1995, “Об участии в международном информационном обмене” от 4.07.1996 и другие. Особо хотелось отметить усилия нашей страны на международной арене[[62]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn62) . В частности, Россия предложила на рассмотрение ООН пакет международных принципов, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем и на борьбу с информационным терроризмом и криминалом. В документе зафиксировано право каждого как на получение и распространение информации, так и на защиту своих информационных ресурсов от неправомерного использования и несанкционированного вмешательства. Кроме того, предполагаетсяя, что государства должны принять меры для ограничения угроз в сфере международной информации. Например, взять на себя обязательства по отказу от действий по нанесению ущерба другим государствам в области информации, по доминированию и контролю в информационном пространстве, по поощрению действий террористических и преступных сообществ, по организации информационных войн, по манипулированию информационными потоками и по информационной экспансии. Согласно предложению России, ООН предстоит определить признаки и классификацию информационных и консциентальных войн, информационного оружия, создать систему международного слежения за выполнением взятых на себя государствами обязательств, создать механизм разрешения конфликтных ситуаций в этой сфере. В документе оговорена также международная ответственность государств за выполнение обязательств и процедура мирного урегулирования споров по информационным проблемам.

К организационно-техническим методам относятся:

\* создание и совершенствование системы обеспечения информационной безопасности страны;

\* разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств;

\* развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;

\* создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

\* выявление технических устройств и программ, представляющих опасность дли нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;

\* сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

\* совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации;

\* контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности;

\* формирование системы мониторинга показателей и характеристик информационной безопасности страны в наиболее важных сферах жизни и деятельности общества и государства.

Одной из технологических тенденций последнего времени стал повсеместный переход на системы многофакторной идентификации, нередко с использованием биометрических данных. Простая комбинация из регистрационного имени и пароля, даже часто обновляемого, уже не обеспечивает требуемого уровня защиты.

Другая тенденция – повышенное внимание не столько к средствам защиты, сколько к инструментам мониторинга и администрирования систем безопасности. Такое смещение акцентов означает интеграцию политики безопасности в процессы управления коммуникациями, в общую информационную стратегию и бизнес-процессы компании.

По данным исследования IDC[[63]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn63) “Russia Security Software 2005-2009 Forecast and 2004 Vendor Shares” российские пользователи затратили в 2004 г. почти 42 млн. долларов на программное обеспечение для систем информационной безопасности, что на 32,7% больше, чем в 2003 г. Наиболее бурный рост IDC отметила в сегментах интегрированных решений и систем 3”А” (аутентификация, авторизация, администрирование), объемы которых увеличились на 58% и 83%, соответственно. Однако, основные затраты пользователей (почти 40%), как и в предыдущие годы пришлись на сегмент управления безопасностью информации. Хотя темпы его роста будут почти вдвое ниже, чем интегрированных решений и систем 3”А”, он останется самым крупным сегментом рынка ПО для систем безопасности, считает IDC. Сам же рынок ПО для систем безопасности и далее будет расти значительно быстрее, чем рынок ПО в целом, и в 2009 г. его объем составит 127 млн. долларов.

Экономические методы обеспечения информационной безопасности включают в себя:

\* разработку программ обеспечения информационной безопасности страны и определение порядка их финансирования;

\* совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации;

\* создание системы страхования информационных рисков физических и юридических лиц.

В России затраты на информационную безопасность составляют всего 0,5% от общих расходов на информационные технологии - в два раза меньше, чем в среднем в мире. Пока во многих случаях обеспечение информационной безопасности сводится к противостоянию конкретным угрозам, а не к принятию общей стратегии обеспечения безопасности, основанной на оценке рисков. В то же время, исследования показывают, что ситуация быстро меняется и руководители коммерческих организаций и государственных структур все чаще ставят вопросы обеспечения информационной безопасности в один ряд с другими жизненно важными задачами.

Отдельно необходимо отметить роль государства в контексте масштабного объединения всех ресурсов общества для создания единого комплекса противодействия информационным угрозам. Аркуилла и Ронфельдт считают, что ключом к построению надежной системы национальной безопасности в информационной сфере должна стать государственная информационная доктрина[[64]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn64) . Эта доктрина - в структурах и процедурах - должна подразумевать, что эффективное противодействие сетевым угрозам включает три высоко взаимозависимых сферы противостояния с фактическими или потенциальными противниками:

-способность вести наступательные действия против структуры и процессов принятия решений врага;

-защита собственных способностей принимать и исполнять решения;

-способность создавать и использовать информацию в собственных целях более эффективно, чем это сможет делать противник.

При этом следует иметь ввиду, что часто требуется применять очень сложные средства для нападения на гораздо менее развитые инфраструктуры противника, при необходимости защищать собственные высокоразвитые системы от относительно простого, но потенциально опасного нападения[[65]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn65) :

Наступательная Сфера:

Из трех указанных направлений, наибольшее внимание в настоящее время принято сосредотачивать на наступательных концепциях, т.к. они меньше скованы ограничениями сложившихся информационных структур и процессов. Передний край сетевых взаимодействий следует переносить в организации, которые являются частью или которые, по крайней мере, тесно вовлечены в деятельность разведывательных сообществ. Эти организации более всего подходят для целей информационной войны. Их внимание следует сосредоточить на разведывательной деятельности и на сбалансированном использовании вражеских информационных источников и потоков.

Защитная Сфера:

Защитные аспекты концепции информационной безопасности более сложны для доктринального оформления как структурно, так и процедурно. Это происходит потому, что удобство и эксплуатационная эффективность в обработке информации обычно подразумевают уязвимость этой информации и процессов принятия решений. Требуется масса усилий, чтобы создать концепцию, в которой эта противоречивость требований безопасности и эффективности была сведена к минимуму.

Сфера использования информации:

Эта область заметно сложнее первых двух, потому что относительная эффективность обработки и структурирования информации и системы принятия решений зависит от тонкой асимметрии между нашими собственными целями, способностями и информационными зависимостями, и таковыми противников. На фундаментальном уровне, конечно же, следует готовиться к противостоянию с высокотехнологичными хорошо оснащенными и организованными противниками, которые будут использовать новейшие разработки в области информационного оружия. Но также необходимо иметь концепции защиты от менее зависимых в информационном плане противников, но обладающих адекватной искушенностью, чтобы понять и использовать этот факт. Проблема стоит очень остро даже если не рассматривать прямые нападения, а сосредоточиться на эффективном использовании информации для принятия своевременных и адекватных решений.

Для достижения доктринальной последовательности и эффективности необходимо разработать, по крайней мере, два концептуальных момента:

Во-первых следует научиться лучше различать “экономическую эффективность” и “результативность”, чтобы всегда знать, что в отношении определенной ситуации или цели не происходит так что “делаются хорошо неправильные вещи”, особенно в контексте долгосрочных перспектив.

Во-вторых, надежная система информационной безопасности требует, чтобы были выявлены четкие различия между иерархическими уровнями познавательного процесса, посредством которых данные и информация вносят вклад в принятие эффективных решений. Суть этих различий - единство “осведомленности” (самый низкий уровень познания), “знания” и “понимания”. Можно “знать” что-что, но не знать его специфических особенностей. Точно так же можно “знать” кое-что даже очень хорошо, но не “понимать” его полного значения.

Вот две основных цели государства в информационной безопасности[[66]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn66) :

- снизить способность противника понимать его собственные обстоятельства, наши обстоятельства, и обстоятельства, которые затрагивают обе стороны при сохранении и увеличении нашей способности для такого понимания

- снизить способность противника эффективно использовать любые преимущества, которых он уже смог достичь, и сохранить и увеличить наши собственные возможности в этом отношении.

Достижение и сохранение преимуществ, накопленных в таком противостоянии должно стать фундаментом для будущего успеха в глобальном масштабе стратегического превосходства. Важно, что упомянутую доктрину нельзя рассматривать как что-то “экзотическое” и отделять ее от управления всеми вооруженными силами.

Следующим после выработки доктрины шагом должно стать обеспечение общественной информационной безопасности. Нужно защищать интересы непосредственно всего общества, бороться за информационную безопасность каждого гражданина, а не избранной группы. Важно понимать и то, что процесс информатизации общества должен быть взят под контроль самим этим обществом. Если не уделить этому повышенного внимания, возможно, что потом что-либо кардинально изменить будет уже невозможно. Каждый человек должен знать, кто и какую информацию собирает, кому и для каких целей она доступна. Необходимо предвидеть развитие процесса информатизации, предупреждать общество об опасных тенденциях и вовремя принимать контрмеры. Всем этим должны заниматься государственные и общественные организации с участием представителей правоохранительных структур.

Прежде всего, важно прекратить утечку информации за пределы России. Отдельные авторы предлагают даже объявить информацию о гражданах и организациях особой собственностью государства и запретить использование такой информации за пределами страны, а также обеспечить несовместимость систем идентификации людей и организаций России с общемировыми и запретить использование этих систем вне России[[67]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn67) .

Под пристальным контролем должна быть информация, собираемая:

· государственными структурами (органами управления, правоохранительными органами, структурами, отвечающими за учет коммерческой деятельности, собственности, доходов, социального положения);

· провайдерами сети Интернет, операторами мобильной связи, крупными сайтами в русском Интернете, в особенности системами поиска, рейтингами, системами статистики, серверами электронной почты;

· различными финансовыми организациями, банками, особенно предлагающими использование кредитных карт;

· транспортными организациями (о передвижении людей, грузов);

· всеми предприятиями о своих сотрудниках, вузами и школами об учащихся, больницами, библиотеками, спортивными организациями о посещающих их лицах.

Если заранее известно, что предотвратить выход такой информации за пределы страны невозможно, например, из-за того, что организация находится за рубежом, то целесообразно ограничить деятельность такой организации на территории России.

Помимо сказанного, необходимо выработать и распространить некие “правила личной информационной безопасности”. Важно, чтобы пользователи Интернета избавились от иллюзии своей полной конфиденциальности. Все граждане должны ясно осознавать опасность заполнения каких-либо неанонимных анкет, тем более что зачастую такие анкеты предлагаются не без злого умысла.

Деятельность СМИ - это вопрос национальной безопасности России. Любая свобода, в том числе и абсолютная свобода слова, может быть реализована без ограничений только в идеальном обществе, в котором каждый гражданин, помимо своих прав, осознает еще и ответственность перед обществом в целом и перед государством. Рост влияния СМК на общественное сознание поднимает вопрос о разработке и внедрении в жизнь механизмов государственного и общественного воздействия на руководство и владельцев СМИ. От введения контроля за широковещательными информационными потоками выиграет каждый человек, освободившись от насильственных манипуляций сознанием. Выиграет и общество в целом, так как резко снизится количество преступлений, психических заболеваний и антиобщественных поступков. Какой будет форма контроля, следует решать специалистам, которые должны при разработке соответствующих законопроектов создать механизм, защищающий эту систему контроля от скатывания в формализм или превращения в карательный орган, уничтожающий любое инакомыслие. Пока этот механизм еще не создан, прогрессивные общественные силы, например Общественная Палата, должны активно требовать от депутатов и членов Правительства принять меры по регулированию телерадиовещания. Депутаты Государственной думы РФ и члены Совета Федерации обязаны как можно скорее привести законодательство в соответствие с требованиями времени, разработать и принять соответствующий Федеральный закон, создать специальные комиссии по телевидению, радиовещанию, электронным СМИ. Важно обеспечить действенные предпосылки административной и уголовной ответственности журналистов и руководителей СМИ за искусственное искажение информации в целях манипулирования сознанием, за умышленное нагнетание общественной напряженности, за дискредитацию официальных органов власти в глазах широких слоев населения.

Параллельно следует вести работу по созданию большего количества федеральных спортивных, познавительных, культурных и патриотических каналов; по ограничению применения рекламы не только по видам рекламируемого товара (например, табака или пива), но и по цели воздействия на потребителя (программирование на пьянство, несознательный образ жизни). Информационные программы должны изменить свой формат, сместив акценты с поиска сюжетов о катастрофах, авариях, стихийных бедствиях, на события, вызывающие положительные эмоции. Необходимо на государственном уровне поддерживать создание таких телевизионных программ, которые выстраивают в сознании граждан социально-ответственную модель поведения, воспитывают патриотизм, высокую нравственность, порядочность, честность. Телевидение должно заряжать жителей страны созидательной энергией, стимулировать на производительный труд, настраивать на духовное и интеллектуальное развитие. Все это залог оздоровления общества, в том числе и его экономики, так как ее основа, ее движущая сила и ее цель – это здоровый, всесторонне развитый, высокодуховный человек.

Итак, предпосылками создания информацоннно защищенного, здорового и прогрессивного общества являются:

1. Создание на высшем государственном уровне масштабной “Концепции национальной информационной безопасности”, ее детальная проработка и максимально эффективная реализация.

2. Мобилезация ресурсов всего общества и использование всех доступных механизмов для формирования по-настоящему свободной, “чистой”, адекватной информационной среды.

3. Масштабная работа по повышению общей образованности каждого отдельного человека. Ликвидация информационной безграмотности и некомпетентности населения.

**Заключение**

Технические достижения информационной эпохи предоставили качественно новые возможности средствам массовой информации и коммуникации, превратили их в мощный инструмент влияния. Характерной особенностью является то, что в информационной среде в интегрированном виде и разнообразных, зачастую довольно причудливых сочетаниях, одновременно функционирует информация, которая адекватно отражает существующий мир, а также деформированная, искаженная информация. Это обусловлено как сложностью самого процесса познания и неполнотой знаний о мире, так и пристрастностью, субъективностью людей, а зачастую - целенаправленным использованием информационных процессов при достижении собственных безнравственных целей и игнорировании наносимого своими действиями ущерба другим людям. Подтверждением данного факта могут служить результаты проведенного в работе анализа роли информационных потоков в функционировании политической системы общества и государства. По сути, выделенные разновидности технологий информационного воздействия воплощают в себе определенные способы трансформации и искажения информационных потоков, в результате чего происходят качественные изменения базовых свойств информации, превращающие ее в реальную силу. Благодаря расширяющимся всемирным сетям опто-волоконных и спутниковых систем, в области распространения информации следует ожидать все новых и новых прорывов, а они, в свою очередь, способствуют появлению новых разработок средств информационного оружия. Это обстоятельство ведет к переосмыслению подходов к коммуникации, а также ряда других социально-психологических процессов и явлений в современном обществе и ставит вопрос об “информационной экологии”, защищающей человека от избыточной и недостоверной информации[[68]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn68) . Государство должно играть значительно более активную роль в обеспечении ясных и справедливых правил взаимодействия в информационном поле, как, например, это осуществляется в области гражданско-правовых отношений. Необходимо правильно скоординировать деятельность законодательных и правоохранительных органов, чтобы одновременно обеспечить прочный правовой фундамент, задающий параметры развития информационной среды, и не сковать это развитие излишней регламентацией.

Жизнедеятельность современного человека реализуется в специфической присущей человеческому обществу информационной среде, имеющей свои закономерности, особенности развития и функционирования. Многочисленными исследованиями было установлено, что без постоянного информационного контакта невозможно полноценное развитие человека и общества в целом. При этом в тени оставался тот факт, что информационно-коммуникативные процессы могут таить в себе опасности, представляющие реальную и все возрастающую угрозу. На человека оказывают огромное влияние количество, объем, содержание и структура поступающей и перерабатываемой информации. Прекращение информационной связи может вызывать различные психические аномалии вплоть до психических заболеваний[[69]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn69) . Постоянная информационная связь с окружающим миром, социальной средой, в которой индивид действует как активный социальный субъект, является одним из важнейших условий самореализации человека как личности. Необходимая информация черпается из непосредственного опыта, личного общения, а также из разнообразных источников информации (книги, радио, телевидение, журналы, газеты, различные информационные системы). Причем закономерностью общественного развития является преобладание и резкое увеличение доли информации, получаемой из информационных источников, нежели из непосредственного опыта и личного общения. Усложнение и динамичность социальных процессов в обществе, влияние происходящих общественных изменений непосредственно на повседневную жизнь человека делают его все более зависимым от потоков средств массовой коммуникации. Все меньше сведений, необходимых для своего социального поведения и жизни в обществе, он может получить, основываясь только на своем повседневном опыте, и все больше - из телевизионных и радио программ, периодических изданий. Особенно ярко это проявляется в формировании мнений по вопросам, которые не находят отражения в его непосредственном опыте, например, об обстановке в других городах, регионах, странах, о политических лидерах, об экономической конъюнктуре. Как отмечают многие исследователи, человек, его повседневная жизнь все больше зависит от массовой коммуникации, которая создает для него своего рода “вторую реальность”, “субъективную реальность”, влияние которой не менее значимо, чем влияние реальности объективной[[70]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn70) .

Все это активизирует потребность людей в социально значимой информации для своей ориентировки в политической и социально-экономической ситуации, заставляет их стать активными потребителями информации, участниками информационно-коммуникативных процессов в нашем обществе. В тоже время, происходящие в условиях бурного развития телекоммуникационных средств и информационной техники, создания качественно новых информационных технологий и систем кардинальные общественные изменения привели к резкому количественному и качественному изменению информационной среды самого социума, в которой приходится действовать людям, функционировать всем общественным и государственным структурам, предприятиям, учреждениям. Эти явления выдвигают информационно-коммуникативные процессы и совокупность разноуровневых информационных факторов на ключевое место в сфере государственного и социального управления обществом. В частности, государство должно стремиться к большей информационной открытости, а также к налаживанию и углублению интерактивного взаимодействия с гражданами, общественными институтами и другими субъектами. Первые шаги в этом направлении делаются посредством реализации “электронного правительства” – в виде расширения информационного присутствия государства путем создания официальных интернет-порталов, интенсификации бизнес- и других процессов путем организации он-лайн сервисов, непосредственного участия в управлении через активный гражданский контроль деятельности чиновников.

В информационной среде, представляющей сложное системное образование, выделяется процессуальная составляющая, и, как наиболее динамичная и изменяющаяся ее часть, - информационно-коммуникативные процессы, которые активно воздействуют на индивидуальное, групповое и массовое сознание. В наибольшей степени непосредственному воздействию информационной среды подвержена духовная сфера общества, деформация и деструктивные изменения которой, в форме психоэмоциональной и социальной напряженности, искаженных нравственных норм и критериев, неадекватных социальных стереотипов и установок, ложных ориентаций и ценностей, в свою очередь, влияют на состояние и процессы во всех основных сферах общественной жизни, в том числе политической, экономической, культурной. Конкретные формы влияния информационной среды на духовную сферу общества выделяются как информационное насилие над социальными субъектами различных уровней общности, системно-структурной и функциональной организации; над индивидуальным, групповым и общественным сознанием, а терминологически в общем виде обозначаются как информационный терроризм. Суть данного понятия отражает процесс воздействия информационно-коммуникативных процессов как динамического компонента информационной среды на фундаментальные основания системы принятия решений отдельных людей, организаций и даже государств. Деятельность каждой такой системы неразрывно связана сетью человеческих взаимоотношений и контактов со множеством других подобных систем, поэтому от решений каждого конкретного человека с его личностными характеристиками, индивидуально-психологическими особенностями, собственным уникальным жизненным и профессиональным опытом, привычками и взглядами зависит судьба и благополучие множества других людей, важные социальные, экономические и политические изменения в обществе[[71]](http://www.bestreferat.ru/referat-406097.html" \l "_ftn71) . В конечном счете, именно совокупность взятых в отдельности индивидов, их индивидуальное сознание, являющееся основой для матрицы сознания общественного, выступает как первичный объект воздействия со стороны информационного терроризма. В контексте осуществления государственного управления особую значимость приобретает комплексный и динамический учет максимально возможного количества характеристик общественного развития. Выбранная стратегия должна постоянно переоцениваться и корректироваться в соответствии с текущим моментом.

Для выводов по предпринятому в работе анализу информационной безопасности следует выделить три главных вектора стратегии развития Концепции национальной информационной безопасности:

Во-первых, создание специальных структур, занимающихся исследованием средств информационного воздействия.

Во-вторых, привлечение специалистов по изучению технологий информационного насилия.

В-третьих, формирование специальных структур и процедур для выявления признаков враждебного использования информационных технологий.

От эффективности деятельности этих структур и используемых защитных процедур зависит информационно-коммуникационная безопасность и нормальное функционирование всех социальных субъектов, в качестве которых выступают граждане, органы власти и государственного управления, общественно-политические и экономические организации.

Также следует отметить, что использование манипулятивных приемов, включая комплексное и массированное их применение, имеет значительно меньший эффект в аудитории высокообразованной, с устойчивой системой обоснованных взглядов, а также знающей технику манипулятивного воздействия и обладающей некоторым опытом целенаправленной социально-психической защиты. Поэтому государство должно отдельно сосредоточиться на интеллектуальном развитии своих граждан.

В последнее время все больше исследователей обращают внимание на необходимость активной разработки проблематики информационной безопасности личности, общества и государства, а также выделения информационной безопасности в качестве самостоятельного предмета теории и социальной практики. Связано это с тем, что процессы и технология воздействия информационной среды на духовную сферу обладают качественной спецификой, которая определяет необходимость рассмотрения этой темы в концептуальном, методологическом и методическом плане. Сама логика общественного развития выдвигает эти проблемы в число первоочередных. Без их решения невозможно дальнейшее устойчивое прогрессивное развитие.