9. *Михайлов А.П.* Математическое моделирование динамики распределения власти в иерархических структурах // Математическое моделирование. 1994. Т. 6. № 6. С. 108–138.
10. *Михайлов А.П.* Моделирование российской власти // Социс. 2001. № 5. С. 12–20.

Grigoryan David Kromvelovich, candidate of political sciences, doctoral candidate, South-Russia Institute of Management – branch of Russian Presidential Academy of National Economy and Public Administration. (70/54, Pushkinskaya St., Rostov-on-Don, 344002, Russian Federation). E-mail: davo-davo23@mail.ru

HIERARCHICAL AND POLIARKHICAL STRUCTURES OF POWER DISTRIBUTION IN THE CONTEXT OF LEADER AND ELITE POSITIONING

Abstract

In article two main ways of representation of the imperious relations are allocated: hierarchical and poliarkhical. Depending on it also the political culture at the elite and basic levels which is shown, respectively, as authoritative or democratic that significantly affects forms of leader and elite positioning is structured.

Keywords: *political culture, leader and elite positioning, hierarchical structure of the power, poliarkhical structure of the power, political leader, political elite.*

УДК 321.74

АКТИВАЦИЯ ИНФОРМАЦИОННОГО КОМПОНЕНТА В ОБЕСПЕЧЕНИИ ВОЕННОЙ БЕЗОПАСНОСТИ

Ковалев Андрей Андреевич кандидат политических наук, доцент кафедры государственного и муниципального управления, Северо-Западный институт управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (199178, Россия, Санкт-Петербург Средний пр., В.О., д. 57/43). E-mail: senator23@yandex.ru

Аннотация

В статье рассматриваются международные методы противодействия информационно-психологической агрессии и информационной войне. Выделены и проанализированы два основных подхода к исследованию этих критериев исходя из технико-технологического и гуманитарного измерений реализации информационной политики государства. Приняв во внимание общепринятое определение информационной безопасности государства как состояния защищенности жизненно важных интересов личности, общества и государства, речь идет о возможности предотвратить вред населению через: неполноту, несвоевременность и недостоверность используемой информации; негативное информационное влияние; негативные последствия информационных технологий; несанкционированное использование, распространение нарушения целостности, конфиденциальности и доступности информации.

Ключевые слова: *информационная безопасность, информационная война, информационная уязвимость, информационное оружие, критерии оценки информационной безопасности.*

Целью данной статьи является определение международных критериев оценки информационной безопасности, выделение и исследование технико-технологического и гуманитарного измерений обеспечения информационной безопасности, анализ международных методов противодействия информационно-психологической агрессии и роли информационной войны в безопасности государства.

Обеспечение военной безопасности современного государства зависит не только от фактического наличия собственного, адекватного вероятному противнику военного потенциала, но и все более базируется на качественно иных факторах, прежде всего носящих экономический, информационный, технологический, политический и социальный характер. В связи с этим аспект обеспечения военной безопасности РФ необходимо рассматривать, как разумный компромисс между потребностями и возможностями государства по поддержанию своих Вооруженных Сил, обеспечивающих ведение военных действий в рамках локальных вооруженных конфликтов и локальных войн и способность военной организации государства обеспечить поддержание стратегической стабильности, контролируемое предотвращение войны, динамическое развитие российского общества, решение всего существующего и потенциального комплекса политических, социально-экономических и других проблем. С развитием глобальных информационно-коммуникационных технологий в конце прошлого века существенно выросли угрозы информационной безопасности, и поэтому возникла объективная настоятельная необходимость разработки новых международных критериев информационной безопасности с целью избегания военных и политических конфликтов. Исходя из общепринятого определения информационной безопасности государства как состояния защищенности жизненно важных интересов личности, общества и государства говорится о возможности предотвратить вред населению через: неполноту, несвоевременность и недостоверность используемой и потребляемой информации; негативное информационное влияние; негативные последствия информационных технологий; несанкционированное использование, распространение нарушения целостности, конфиденциальности и доступности информации. При этом, по мнению ученого А.Чичановского, важным является сохранение сбалансированности интересов личности, общества и государства [16, с. 352]. Если интересы личности состоят в реализации конституционного права доступа к информационным ресурсам и не запрещенного законом их использования, а также защиты персональных данных, то интересы общества заключаются в достижении общественного согласия и духовного развития общества на основе обеспечения интересов личности, в укреплении демократии, построении правового государства и формировании концепции безопасной страны. Государство, в свою очередь, крайне заинтересовано в развитии национальной информационной инфраструктуры, реализации гражданами конституционных гарантий права доступа к информационным ресурсам для сохранения незыблемости конституционного строя, суверенитета и территориальной целостности государства, военной, социально-политической и экономической стабильности.

В соответствии с национальными интересами государства формируются внутренняя и внешняя политика по обеспечению информационной безопасности, что требует более совершенных систем и технологий управления - информационных технологий

(ИТ). Одной из таких технологий, очевидно, являются современные информационные войны. Впервые на научном уровне этот вопрос поднял известный исследователь Э. Тоффлер, утверждая, что «для цивилизации третьей волны одним из главных видов сырья будет информация» [14, с. 33]. Исходя из того, что все виды ресурсов цивилизации делятся на материальные и нематериальные. Информационную безопасность целесообразно рассматривать и исследовать в двух измерениях: технико-технологическом и гуманитарном.

В технико-технологическом измерении методологической базой для определения требований защиты информационных систем от несанкционированного доступа, создания защитных систем и оценки степени защищенности существуют критерии оценки информационной безопасности. Главной задачей таких стандартов информационной безопасности является согласованность позиций и запросов трех групп специалистов, которые в равной степени их используют, - производителей, потребителей и экспертов по квалификации уровня безопасности. Если для производителей в первую очередь важна максимальная конкретность стандартов и общие требования критериев, то для потребителей определяющими являются простота критериев и однозначность параметров выбора защищенной системы.

Начало выработки стандартов информационной безопасности, по убеждению подавляющего большинства исследователей, заключен в 1983 году так называемой «Оранжевой книгой» Министерства обороны США - «Критерии оценки надежных компьютерных систем». Согласно этому документу безопасной является информационная система, которая управляет доступом к данным, однако абсолютно безопасных систем не существует. Следовательно, целесообразно оценивать степень доверия к системе, ее надежность. В 1986 г. страны Европы совместно разработали общие «Европейские критерии безопасности информационных технологий» [6, с. 390], которыми, в частности, были определены задачи средств информационной безопасности. Для определения эффективности и надежности средств защиты в еврокритерии впервые введено понятие «адекватности средств защиты» и определено семь уровней адекватности: по возрастанию - от Е0 до Е6.

Если первый стандарт информационной безопасности - «Оранжевая книга» - предназначался для систем специального и военного потребления, то сфера применения разработанных несколькими годами позже еврокритериев значительно расширена. В этот стандарт вошли: распределенные системы, сети, системы телекоммуникаций и системы управления базой данных. Разработанные в 1993 г.. «Канадские критерии безопасности компьютерных систем» сферой своего применения рассматривают все типы компьютерных систем. С целью создания единого международного стандарта информационной безопасности совместными усилиями авторов «Европейских критериев безопасности информационных технологий», «Федеральных критериев безопасности информационных технологий России» и «Канадских критериев безопасности компьютерных систем» в 1996 завершена работа по объединению этих стандартов в «Единые критерии безопасности информационных технологий» (англ .: Common Criteria for Information Technology Security Evaluation), которые провозглашены неотъемлемым компонентом информационных технологий.

Согласно «Единственным критериям» для характеристики основных критериев информационной безопасности применяется модель триады CIA (англ .: CIA Triad), которая предусматривает три основные характеристики информационной безопасности: конфиденциальность, целостность и доступность (англ. Confidentiality, Integrity and

Availability (CIA)). Возможность несанкционированного ознакомления с информацией считаются угрозами конфиденциальности. В случае, если существуют требования к ограничению возможности модификации информации, их относят к критериям целостности. Угрозы, принадлежащих к нарушению возможности использования компьютерных систем или обрабатываемой информации, составляют угрозы доступности. Идентификация и контроль действий пользователей, управляемость компьютерной системой является предметом наблюдаемости и управляемости. Информационные системы анализируются в трех главных секторах: технических средствах, программном обеспечении и коммуникациях для идентификации и применения промышленных стандартов информационной безопасности как механизмы защиты и предотвращения на трех уровнях: физическом, личном и организационном.

«Единые критерии», по мнению исследователей О.Петрова, О.Таликина и А.Минина [7, с. 92], позволяют с помощью механизмов профилей защиты: потребителям - создавать частные комплексы требований, соответствующих их потребностям; разработчикам - использовать в качестве основы для создания спецификаций своих продуктов. По убеждению ученых, главные преимущества «Единых критериев» – полнота требований информационной безопасности, гибкость в применении и открытость для дальнейшего развития с учетом новейших достижений науки и техники.

Наиболее удачным, на наш взгляд, определением технико-технологического измерения информационной безопасности и защиты информации является «защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий естественного и искусственного характера, в результате которых наносятся убытки владельцам или пользователям информации и инфраструктуре, которая их поддерживает [5, с. 13]. Информационная безопасность обеспечивается за счет защиты информации». В свою очередь, защитой информации является комплекс мероприятий, направленных на обеспечение необходимого уровня информационной безопасности.

Современный уровень развития цивилизации, по мнению Г.Почепцова, является причиной того, что «информация несет в себе как творческую, так и разрушительную силу, но в гораздо большей степени, чем это было раньше» [8, с. 79]. Следовательно, наряду с безопасностью информационных технологий и информационных ресурсов не менее важным, на наш взгляд, является гуманитарное измерение информационной безопасности, то есть защита информации и информационная уязвимость личности, общества, государства, цивилизации. Использование новых прогрессивных информационных технологий в общественной жизни, производстве и управлении, оборонной сфере, возможности быстрого обмена научно-технической, экономической, учебной и другой информации является подтверждением значимости информации как системообразующего социального явления. В то же время общество, по мнению современных исследователей, «с большим опозданием начинает осмысливаться политические, экономические, социальные, военные, психологические и другие последствия глобальной информатизации» [5, с. 11]. Очевидно, что технологически развитые государства пытаются и будут продолжать увеличивать политическое, экономическое и военное преимущество за счет достижения преимуществ в уровне информатизации; и, как следствие, - установление и проведение глобального информационного контроля над менее развитыми государствами, проведение в общем информационном пространстве идеологической и культурной экспансий.

Информационные войны велись постоянно с древних времен и в большинстве случаев производили существенное влияние на становление и развитие различных государств. Однако именно термины «информационная война», «информационная операция» начали активно использоваться в 1991 г. после военного конфликта в Персидском заливе. Ярким и действенным примером успешного ведения информационной атакующей войны, ее влияния на конечный результат, по мнению специалистов, была война в Ираке, получившая название «Буря в пустыне», где новые информационные технологии впервые были применены в военных целях. Первым официальным документом по этому поводу, по мнению ученых, была официальная директива министра обороны США № TS 3600.1 от 21 декабря 1992 «Информационная война», результатом которой через год стала директива Комитета начальников штабов Министерства обороны США № 30-93, в которой информационную войну определено как «комплексное проведение по единому замыслу и плану психологических операций, мероприятий по оперативной маскировке, радиоэлектронной борьбе и физическом уничтожении пунктов связи с целью лишения противника информации, вывод из строя или уничтожение его систем управления при одновременной защите своих сил от аналогичных действий» [4, с. 41]. Этот документ, по оценке специалистов, стал отправной точкой для дальнейших как военных, так и государственных документов и исследований не только в США, но и в других странах мира [3, с. 425]. С 1994 гг. в США проходят официальные научные конференции по вопросам информационных войн и создан Центр информационной стратегии и политики, главной задачей которого является изучение возможностей использования информационных технологий в военных конфликтах XXI века. В 1995г. Сотрудники корпорации RAND провели военные игры «Бой без поля боя - война в XXI веке» [2], в которых принимали участие ведущие специалисты США в области компьютерной безопасности из корпораций, государственных организаций и Министерства обороны США. На этих играх отрабатывались вопросы выработки стратегий защиты США в случае использования противником средств информационной войны. Как потенциальный враг рассматривался Иран. В дальнейшем во всех вооруженных конфликтах с участием США были задействованы различные виды информационного оружия.

К информационному оружию, по определению ученых А. Чичановского и О. Стариша, принадлежат специальные средства, технологии и данные, помогающие влиять на информационное пространство общества и наносить ущерб жизненно важным интересам государства [4, с. 414]. Информационное оружие определяется комплексом средств, предназначенных для:

- воздействия на информационные системы противной стороны;
- внедрение в компьютерные сети систем управления и телекоммуникаций соответствующих элементов и программного обеспечения, которые искажают данные;
- управление поведением людей путем воздействия на их сознание с помощью системы средств массовой коммуникации.

До сих пор термин «информационная война» имеет дискуссионный и неоднозначный характер, несмотря на то, что разные авторы трактуют его по-разному, в зависимости от того, какие аспекты проявлений и содержания они исследуют. Например О.Дубас условно разделяет исследователей информационных войн на три основные группы [4, с. 69]: тех, кто предпочитает социально-коммуникативный подход, понимает информационную войну как отдельные информационные мероприятия, информационные способы и средства как корпоративной конкуренции, так и ведения межгосударственного противоборства, вооруженной борьбы, коммуникационные технологии воздей-

ствия на массовое сознание. Ко второй группе исследователей входят, в основном, представители военных ведомств, которые рассматривают информационную войну через призму военного противоборства и считая её комплексным совместным применением сил и средств информационной и вооруженной борьбы (военно-прикладной подход). По мнению третьей группы ученых, информационная война - это явление мирного периода межгосударственного противоборства, которое позволяет решать внешнеполитические задачи с помощью не силовых, в традиционном понимании, методов.

По убеждению И.Горбатенко, В.Долгова, Т.Гриненко, информационная война является противоборством непримиримых сторон в соответствующем информационном пространстве, которое осуществляется с использованием информационного оружия с целью нанесения максимальных потерь «противнику» и минимизации личных потерь в экономической, военной, политической и идеологической сферах [3, с. 11].

Один из первых теоретиков информационных противоборств Мартин Либики определяет семь форм информационной войны [16, с. 408]:

- борьба с системой управления и коммуникаций противника;
- борьба за информацию о собственных силах и силе противника для получения решающего стратегического превосходства над противником;
- радиоэлектронная борьба;
- борьба с гуманитарными системами противника;
- борьба с технико-технологическими системами противника;
- блокирование или направления данных об экономическом состоянии в нужное русло для экономического доминирования.

Замечая, что единственным компонентом, присутствующим во все этапах информационной войны, является борьба с гуманитарными системами противника, то есть психологическая война, ученый дифференцирует психологическую войну на отдельные сегменты, а именно:

- операции против национального самосознания;
- операции против руководства стороны противника;
- операции против войск противника;
- культурные конфликты.

При этом он отмечает, что сторона, которая собирается манипулировать другой с помощью средств массовой коммуникации, прежде всего должен определить целевые аудитории противной стороны. Важнейшая задача на подготовительном этапе информационного противоборства, по мнению аналитиков, является использование возможностей средств массовой коммуникации для: введения в заблуждение потенциального противника, планомерной дискредитации его военно-политического руководящего состава и лидеров, ограничения информационно-пропагандистского функционирования противника вплоть до организации тотальной информационной блокады.

Безусловно, пытаясь получить преимущество в различных сферах, технологически развитые государства будут пытаться влиять на другие государства. Так, «борьба культур», по мнению М.Либики, не будучи формой вооруженного противоборства, ставит своей задачей культурную экспансию, облегчая тем самым применение психологического оружия и, что самое главное, позволяет точнее спрогнозировать результаты этого применения. Еще одной чертой конфликтов современности стало стремление к интеллектуальному доминированию, в отличие от физического доминирования в прошлом. Желание победить противника не воюя, или лишить его возможности сопротивляться, привело к еще одной форме информационной войны - экономическому доми-

нированию. Объединение методов информационной и экономической войн, по мнению ученого, приводит такие формы противоборства, как блокирование сведений об экономической мощи и информационный империализм, который облегчает транснациональным корпорациям, которые на сегодняшнем этапе потеряли национальные признаки, вести борьбу за экономическое доминирование, в том числе и провоцируя военные конфликты в регионах своих корпоративных интересов.

С помощью комплексного подхода, А.Фисуном предпринята попытка вывести синтетическое понятие: информационная война - это комплексный открытый или скрытый арсенал целенаправленного информационного воздействия одной стороны, или взаимное влияние сторон друг на друга, который охватывает систему методов и средств воздействия на людей, их психику и поведение, на информационные ресурсы и системы с целью достижения информационного превосходства в обеспечении национальной, способной привести к принятию намеченного инициатором воздействия решений, или тотально парализовать информационную инфраструктуру противника с одновременным планомерным укреплением и собственной защитой информации и информационных систем [15, с. 46]. Информационная война предполагает нарушения, повреждения, модификацию информационных ресурсов и знаний, и представлений людей о самих себе и окружающем мире и влияет на общественное мнение и мнение элит, меры дипломатического характера, пропагандистские и психологические кампании, целенаправленные подрывные акции в области культуры и политики, дезинформацию и внедрение в местные медиа-каналы, несанкционированное проникновение в компьютерные сети и базы данных, техническое содействие диссидентским и оппозиционным движениям и предоставление им информационной поддержки. С развитием технических средств, увеличивается число приемов ведения информационной войны: от «информационной борьбы первого поколения», существовавшей в форме расширенной классической радиоэлектронной борьбы, к «информационной борьбе третьего поколения», под которой понимаются операции на основе эффектов [1]. Операции на основе эффектов сегодня является основой реализации внешнеполитической деятельности развитых государств в современной информационной эпохе. Основополагающим аспектом информационного противоборства было и остается стремление к информационному преимуществу.

Военная политика современного государства и военно-политические процессы детерминированы сложным комплексом причин и факторов, порождающих серьезные противоречия политической динамики, как во внутренней, так и во внешней сфере. Среди особенностей военно-политического процесса в РФ выделяются: синкретизм политики и экономики, социальных и личных отношений; отсутствие консенсуса между непосредственными участниками военно-политического жизни; активный политический стиль, состоящий в навязывании обществу часто разновекторных нововведений; концентрация политической власти и ресурсов в руках правящей элиты.

Уже в первых постсоветских исследованиях проблем обеспечения безопасности Российского государства подчеркивалось необходимость комплексной деятельности по «снятию» внешних и внутренних угроз его устойчивому функционированию и развитию, позволяющему выступать России в качестве суверенного субъекта межгосударственных отношений, а также гарантировать возможность стабильного всестороннего прогресса всему обществу в целом и каждому его члену в отдельности [9, с.12].

Военная безопасность - важнейшее направление военной политики и стратегический компонент национальной безопасности России, которые определяют состояние

обороноспособности страны и возможности по обеспечению защиты национальных интересов. Исследователи военную безопасность рассматривают по-разному. Так, профессор И. Радиков определяет ее как «состояние жизнедеятельности социума, его структур и институтов, гарантирующее их качественную определенность в параметрах надежности существования и устойчивости развития посредством исключения военного насилия [11, с. 81-82]. Другим исследователем, военная безопасность рассматривается как «особое состояние отношений между государствами (или их коалициями), обусловленное сочетанием политических, экономических, военных и других факторов, исключающих возможность начала войны (военных действий)» [6, с. 39]. Таким образом, военная безопасность - это способность государства целенаправленно и контролировано противодействовать возникновению войны, потенциальному вовлечению в войну, а в случае ее фактического возникновения - сведения к минимуму ущерба и разрушительных последствий для национальной безопасности страны. Требуемый уровень достигается при использовании комплекса структурных компонентов: военных, политико-дипломатических, экономических, гуманитарных и других, целенаправленными усилиями государственных и политических институтов.

С целью эффективного, планомерного и контролируемого обеспечения целостной военной безопасности России необходимо функционирование по единому замыслу системы военной безопасности, которая выражается в эффективной деятельности трех компонентов: управленческий, силовой и обеспечивающий. Система обеспечения военной безопасности должна не только реагировать на угрозы и вызовы, но и обладать предвидением возможных угроз. Основополагающим фактором требований к системе обеспечения военной безопасности является сочетание централизованного и децентрализованного управления средствами обеспечения военной безопасности в соответствии с устройством России.

Конкретные требования к системе обеспечения военной безопасности определяются характером военных угроз. Поэтому согласимся с позицией И. Радикова, утверждающим, что «перемещение военных действий в информационное пространство повлекло за собой появление в военной доктрине Российской Федерации 2014 года пункта об использовании информационных и коммуникационных технологий в военно-политических целях для противодействия акциям, противоречащим международному праву, направленным против суверенитета, политической независимости, территориальной целостности государств и представляющим угрозу международному миру, безопасности, глобальной и региональной стабильности [10, с.45].

К первоочередным задачам модернизации военной организации РФ следует отнести:

- совершенствование организации военного планирования;
- оптимизация структурной компоненты и мест дислокации войск; готовность к защите информационной инфраструктуры, информационных систем стратегических и критически важных объектов, к противодействию информационной пропаганды направленной в военную сферу; техническое переоснащение Вооруженных Сил; повышение качества допризывной подготовки;
- в информационной сфере важное место должны занимать разработка принципов государственной информационной политики, укрепление государственных средств массовой информации, развитие информационных технологий, осуществление информационной и культурной экспансии в отношении зарубежных стран.

Таким образом, обеспечение военной безопасности страны – это важнейшее направление военной политики России. В новых военно- политических концепциях все большее место занимают суждения о том, что война и военная сила не является самым эффективным инструментом политики. По многим мнениям считается, что безопасность невозможно обеспечить только военными средствами. Поэтому основной упор в разрешении конфликтов необходимо делать на политические средства и дипломатические усилия.

Военно-политическая деятельность представляет собой непосредственные усилия субъектов военной политики по формированию желательной для них военно-политической обстановки. В зависимости от характера решаемых задач она подчинена либо предотвращению войны, развитию мер доверия, либо подготовке к военной экспансии. Деятельность государства по предупреждению, срыву или отражению вооруженного нападения, обеспечению своей безопасности военными методами соответствует нормам международного права [1].

Следующим важным аспектом, связанным с формированием и обеспечением реализации государственной информационной политики является отнесение обеспечения информационной безопасности в важнейшей функции государства, которая должна предусматривать, прежде всего, формирование соответствующими государственными органами политики и правовые механизмы ее реализации в области информационной безопасности. Важная роль в этом направлении деятельности принадлежит государственным органам, которые в соответствии с предоставленными полномочиями в сферах своей ответственности должны осуществлять организационное, нормативно-правовое, методическое, научно-технологическое, материально-техническое и финансовое обеспечение реализации государственной политики информационной безопасности.

Необходимо отметить, что даже краткий анализ отечественных и зарубежных нормативно-правовых актов позволяет сделать вывод об актуализации путей совершенствования информационной безопасности и упорядочения информационных отношений во всех сферах жизнедеятельности общества и функционирования государственных и негосударственных учреждений. Так, нестабильная геополитическая политическая ситуация в современном мире активизирует разработку, внедрение и реализацию мероприятий, направленных на обеспечение информационной безопасности.

Только системное, комплексное и целенаправленное выполнение возложенных мероприятий всеми субъектами будет способствовать повышению эффективности реализации государственной политики в сфере информационной и военной безопасности РФ.

Выводы. Теоретико-методологический анализ международных критериев информационной безопасности позволяет выделить два основных подхода к исследованию этих критериев. В рамках первого подхода рассматривается технико-технологическое измерение информационной безопасности. Информационная война понимается как противоборство информационно-коммуникационных технологий и способности государственных и коммерческих информационных систем обеспечить безопасность инфраструктуры государства в целом. К технико-технологическому измерению, на наш взгляд, следует отнести такие международные критерии информационной безопасности:

- защита информационных ресурсов от несанкционированного доступа с целью обеспечения конфиденциальности;

- обеспечение целостности информационных ресурсов путем их защиты от несанкционированной модификации или уничтожения;
- обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании.

Второй подход исходит из гуманитарного измерения информационной безопасности и описания явления информационной войны через ее влияние на массовое сознание, манипулятивный потенциал и психологическое воздействие информационных сообщений. К международным критериям информационной безопасности гуманитарного измерения, в частности, относятся:

- защита собственной информации и информационных систем;
- противодействие негативному влиянию на человеческое сознание с помощью системы средств массовой коммуникации;
- защита информационных ресурсов и знаний людей о самих себе и окружающем мире;
- противодействие пропагандистским и психологическим кампаниям, подрывным акциям в области культуры и политики.

Под термином военная безопасность мы понимаем особое состояние отношений между государствами (или их коалициями), обусловленное сочетанием политических, экономических, военных и других факторов, исключающих возможность начала войны (военных действий).

В условиях информационной войны объектами разрушения становятся ценностные ориентиры общества, национальный менталитет, общественный идеал, а одним из основных инструментов деструктивного информационного воздействия становятся средства массовой коммуникации. Таким образом, проблема государственного обеспечения информационной безопасности личности и общества имеет комплексный характер и для ее решения требуется системное исследование и планирование.

Литература

1. *Бельков О.А.* О понятийно-категориальном аппарате теории и политики национальной безопасности России. // Экспертно-аналитическое обозрение «Безопасность России-2010». – М.: Наука-XXI, 2010.
2. Бой без поля боя - война в 21 веке [Электронный ресурс] / (По материалам корпорации RAND). - Режим доступа: http://www.wplus.net/~kvn/gensec.htm
3. *Горбенко И.Д., Долгов В.И., Грененко Т.А.* Информационная война – сущность, методы и средства ведения: материалы юбилей. научно-технич. конф. – М., 1998. – С. 11-14.
4. *Дубас А.П.* Информационная война: новые возможности политического противоборства // Образование региона. - 2010. - № 1. - С. 69-72.
5. *Жуков В.* Взгляды военного руководства США на ведение информационной войны // Зарубежное военное обозрение. - 2001. - № 1.
6. *Ковалев А.А.* Властные механизмы обеспечения военной безопасности Российской Федерации : дис. ... канд. полит.наук: 23.00.02 / Ковалев Андрей Андреевич. - СПб., 2015. - С.39.
7. *Петров А.С., Талыкин А.А., Минин А.В.* Критерии оценки защищенности информации в компьютерных системах: сочетание единых критериев и критериев // Вестн. Восточно-укр. нац. ун-та им. В. Даля. 2005. № 1.

8. *Почепцов Г.Г.* Информационные войны. – М.: Ваклер, 2000.
9. *Радиков И.В.* Военно-политические проблемы обеспечения безопасности Российского государства в переходный период: дис. ... канд. филос.наук: 09.00.10 / Радиков Иван Владимирович. - М., 1992.
10. *Радиков И.В.* Новая сущность войны в XXI веке и ее отражение в военной доктрине Российской Федерации // Вестник Санкт-Петербургского университета. Серия 6: Философия. Культурология. Политология. Право. Международные отношения. 2015. № 2. С. 39-51.
11. *Радиков И.В.* Военная безопасность общества и государства: Политологический анализ: дис. ...д-ра полит.наук: 23.00.01 / Радиков Иван Владимирович. - СПб., 2000. - С. 81-82.
12. *Расторгуев С. П.* Информационная война. - М.: Радио и связь, 1999.
13. *Рубан В.Я.* Информационная безопасность: сущность и проблемы // Стратегическая панорама. 1998. № 3-4. С. 12.
14. *Тоффлер Э.* На пороге будущего // «Американская модель»: с будущим в конфликте. - М., 1984.
15. *Фисун А.А.* Теоретически-категориальное осмысление понятия «информационная война» в структуре информационно политического пространства / А. Фисун // Информационное общество. 2011. Вып. 13. С. 43-48.
16. *Чичановский А.А.* Информационные процессы в структуре мировых коммуникационных систем: учебник. - М.: Грамота, 2010. 568 с.

Kovalev Andrey Andreevich, candidate of political sciences, associate professor of the public and municipal administration, Northwest institute of management of Russian Presidential Academy of National Economy and Public Administration (57/43, Sredny Ave., V.O., St. Petersburg, 199178, Russian Federation). E-mail: senator23@yandex.ru

ACTIVATION OF INFORMATION COMPONENT IN ENSURING MILITARY SAFETY

Abstract

This article investigates methods to counter international information and psychological war of aggression on the basis of theoretical and methodological analysis of international criteria of information security. Isolated and analyzed two basic approaches: technical and technological and humanitarian measure implementation of the information policy of the state to ensure the information security of the individual, society and state. Based on the generally accepted definition of information security of the state as the state of protection of the vital interests of the individual, society and the state, it is a way to prevent damage to the population through: incomplete, untimely, and unreliable information used , the negative impact of information, the negative effects of information technology; unauthorized use, distribution, and violation of the integrity, confidentiality and availability of information.

Keywords: *information security, information warfare, information vulnerability, information warfare, information security evaluation criteria.*