**ПАЩЕНКО А.С.**

*преподаватель кафедры защиты информации ВИИРЭиС, города Алматы*

**СПОСОБЫ ВЕДЕНИЯ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА В ВОЕННЫХ КОНФЛИКТАХ**

**Аннотация.** Настоящая статья посвящена исследованию теории и практики организации и проведения операций информационной и психологической войны в средствах массовой информации и коммуникации, в том числе в сети Интернет. Объектом настоящего исследования являются виды современного информационного противоборства (включающие в себя информационные войны и психологические операции), предметом – формы и методы их применения в конкуренции между государствами, в международных отношениях и мировой политике. Цель исследования – выявить особенности ведения современных информационных войн и организации психологических операций. Методологической основой исследования является структурно-функциональный подход, методы анализа, синтеза, индукции, дедукции, систематизации, включенного наблюдения. Автор обращает внимание на то, что современная информационная война – это межгосударственный конфликт, возникающий на этапе осознания и обострения политических противоречий между будущими антагонистами (в роли которых могут выступать государства и политические элиты), формирующий будущую структуру конфликтных отношений и создающий условия для применения одним из антагонистов прямой вооруженной силы. Информационная война – это особая стадия политического (международного) конфликта, охватывающая предварительную и подготовительную фазы развития вооруженного конфликта. Структурно информационная война состоит из последовательности информационных операций, а сами операции – из последовательности информационных атак, согласованных по целям, задачам, объектам и времени информационного воздействия. В современных международных отношениях и мировой политике операции информационной войны планируются не шаблонным способом, а ситуативно, с применением множества разнообразных схем, приемов и подходов. При этом эффективность операций информационной войны часто зависит не столько от избранных способов и методов информационного воздействия на противника, сколько от ширины и синхронности охвата этим воздействием массовых аудиторий, то есть – от каналов доведения управляющего информационно-психологического воздействия до сознания конкретных граждан.

**Ключевые слова:** политическая система, Россия, мировая политика, внешняя политика США, международные отношения, дипломатия, международные конфликты, государство, безопасность, США

Информационная война как особое явление в международных отношениях и мировой политике приобрел заметную значимость с развитием телекоммуникационных систем, особенно – сети Интернет. Это связано с третьей промышленной революцией (информационной) и становлением информационного общества, повсеместной компьютеризацией, а также вовлечением все большего числа людей в обмен, распространение и, собственно, создание информации. Существует множество подходов к рассмотрению информационного общества, какими характеристиками оно обладает, существует ли оно в принципе, но, в независимости от этого, информация на сегодняшний день занимает одну из главенствующих позиций в современном мире.

Развитие социальных сетей позволило распространять информацию практически мгновенно, и, кроме того, появилась возможность транслировать прямые репортажи с места событий без специального оборудования – достаточно иметь при себе телефон и приложение «Periscope». Теперь практически у каждого новостного отдела есть свой аккаунт в социальных сетях, особенной популярностью пользуется социальная сеть «Twitter», поскольку представляет наибольшее удобство в публикации коротких новостных сообщений и молниеносного распространения посредством «хэштегов» и «ретвитов». Но в этой связи образуется самая большая и актуальная проблема на данный момент – достоверность информации.

Здесь существует ряд определенных проблем: во-первых, недостоверность или неофициальность самих источников, во-вторых, недостоверность информации, и, в-третьих, целенаправленное манипулирование информацией официальными и неофициальными источниками.

Эти проблемы тесно связаны с понятием информационных войн, которые из локальной борьбы за популярность между двумя новостными ресурсами сегодня переросли в противостояние различных стран на международной арене.

Прежде чем непосредственно перейти к понятию информационная война, сначала необходимо рассмотреть, что такое информация. По словарю С.И. Ожегова [[1]](http://e-notabene.ru/wi/article_21896.html#1), она представляет собой сведения об окружающем мире и протекающих в нём процессах, воспринимаемые человеком или специальным устройством, а также теорию информации. С середины ХХ века под информацией [[2]](http://e-notabene.ru/wi/article_21896.html#2) стали традиционно понимать общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом; обмен сигналами в животном и растительном мире, а также одно из основных понятий кибернетики.

Еще Н.М. Ротшильд отмечал: «Кто владеет информацией, тот владеет миром». И сегодня не только обладание определенными знаниями может сыграть решающую роль в победе, но куда большее значение приобретает манипуляция информацией и использование ее для управления людьми. Феномен массового человека, который рассматривает в своей работе «Восстание масс» Х. Ортега-и-Гассет [[3]](http://e-notabene.ru/wi/article_21896.html#3), свидетельствует о том, что все сферы жизни современного общества сегодня находятся под властью масс. Массовый человек отличается тем, что лишен умения критически мыслить, обычно следует за остальными и мыслит стереотипами. И такими людьми легко управлять в собственных целях, выдавая им ложную информацию за действительную, что мы и можем наблюдать в реалиях современного мира. Но это имеет масштабные последствия, если говорить о международной арене: здесь любая провокация или манипуляция может иметь различные последствия - от манифестаций до вооруженного конфликта. И сегодня «деятельность, направленная на достижения информационного превосходства, поддержку национальной военной стратегии с помощью воздействия на информацию и информационные системы противника при одновременном обеспечении безопасности и защиты собственника информации» именуют информационной войной [[4]](http://e-notabene.ru/wi/article_21896.html#4).

Безусловно, информационные войны существовали и до развития телекоммуникационных средств и их популяризации, однако методы, средства и характер воздействия в «доинформационную» эпоху были совершенно другие, роль информационной войны в рамках общей борьбы между государствами была скорее вспомогательной, нежели ведущей. Сам же термин «информационная война» появился сравнительно недавно - приблизительно в 70-х годах двадцатого века в работе Томаса Рона «Системы оружия и информационная война» [[5]](http://e-notabene.ru/wi/article_21896.html#5). С тех пор смысловое содержание этого понятия непрерывно меняется, эволюционирует, приобретает новое звучание и новые смыслы.

На сегодняшний момент в научной литературе наиболее часто используются такие определения информационной войны (далее - ИВ), как:

1. ИВ – это «межгосударственное военное противоборство, осуществляемое преимущественно или исключительно путем программно-технического, радиоэлектронного и физического поражения военной и гражданской информационной инфраструктуры государства-противника, дезорганизации его систем государственного и военного управления, дезориентации военно-политического руководства, оказания управляющего информационно-психологического воздействия на личный состав армии и гражданское население, как государства-противника, так и его союзников и соседних государств, при одновременной защите собственных аналогичных объектов» [[6]](http://e-notabene.ru/wi/article_21896.html#6).

2. ИВ – это «коммуникативная технология по воздействию на информацию и информационные системы противника с целью достижения информационного превосходства в интересах национальной стратегии, при одновременной защите собственной информации и собственных информационных систем» [[7]](http://e-notabene.ru/wi/article_21896.html#7);

3. ИВ – это новый способ осуществления вооруженных конфликтов, в которых столкновение сторон происходит в форме психологичсеких операций с применением информационного оружия.

Все три подхода к определению информационной войны, на наш взгляд, лишены универсальности и недостаточно точно отражают суть и природу столь сложного социально-политического явления. Так, информационные войны ведутся как в военное, так и мирное время; следовательно, они не могут быть частью «межгосударственного военного противоборства», как того требует первый подход.

Целью информационной войны не может являться «достижение информационного превосходства в интересах национальной стратегии», как того требует второй подход, так как в этом случае теряется смысл включения в определение ИВ понятия «война». Главная цель любой войны – не достижение абстрактного «превосходства», а вполне конкретное нанесение противнику военного поражения. Если же цель ИВ – «превосходство», то тогда следовало бы переименовать информационную войну в информационную политику.

Что касается третьего подхода, то с его авторами и сторонниками, в принципе, можно было бы согласиться (прежде всего, в том, что ИВ – это вооруженный конфликт, ведущийся странами-участниками в форме психологических операций с применением информационного оружия), если бы в научной среде существовали устойчивые и общепринятые определения как психологических операций, так и такого объекта как информационное оружие.

С моей точки зрения, современная информационная война – это межгосударственный конфликт, возникающий на этапе осознания и обострения политических противоречий между будущими антагонистами (в роли которых могут выступать государства и политические элиты), формирующий будущую структуру конфликтных отношений и создающий условия для применения одним из антагонистов прямой вооруженной силы. Информационная война – это стадия, охватывающая предварительную и подготовительную фазы развития вооруженного конфликта; после перехода конфликтных отношений в фазу прямого (лобового) столкновения информационная война теряет свое самостоятельное значение и становится сервисной функцией войны традиционной.

Структурно информационная война может подразделяться на следующие составные части [[8]](http://e-notabene.ru/wi/article_21896.html#8):

- психологические операции (операции прямого действия);

- дезинформация;

- радиоэлектронная война;

- защита собственной информации;

- физическое разрушение элементов информационных систем противника;

- информационная атака (или информационный «вброс», такой, как был в скандале с «панамскими офшорами»).

Следует отметить, что, помимо понятия «информационная война», в научной среде, в военной сфере и в политике используют также ряд смежных терминов и определений: «информационные операции», «кибервойна», «информационное противоборство», «информационно-психологическая война». Такое разнообразие получилось в результате специфической трактовки исходного американского термина «Information Warfare», который, в зависимости от качества перевода, может звучать и как «информационная война», и как «информационное противоборство». На этом основании многие ученые и специалисты, такие. Например, как А.В. Манойло [[6]](http://e-notabene.ru/wi/article_21896.html#6), ставят знак равенства между информационной войной и информационным противоборством. Вместе с тем, существует и другая точка зрения, согласно которой информационная война, психологическая война, кибервойна и информационное противоборство – не тождественные понятия (такой точки зрения придерживаются, в частности, В.И. Слипченко [[9]](http://e-notabene.ru/wi/article_21896.html#9), И.Н. Панарин [[10]](http://e-notabene.ru/wi/article_21896.html#10) и ряд других ученых). В целом, можно констатировать отсутствие единства в понимании природы, сущности и содержания информационной войны, а также склонность различных авторов к частому использованию множества синонимически близких терминов и определений (на что весьма верно указал А.В. Манойло [[6]](http://e-notabene.ru/wi/article_21896.html#6)), которые следовало бы свести к двум-трем основным категориям: информационной войны, информационной борьбы и стратегической коммуникации. По нашему мнению, стратегическая коммуникация может служить рамочных (общим) понятием и для ИВ, и для различных форм информационной борьбы, не ограничиваясь, впрочем, только ими одними.

Обобщая существующие определения информационной войны, можно выделить ряд специфических черт, которые данной войне присущи:

- объектом ИВ является массовое и индивидуальное сознание;

- в ходе ИВ происходит навязывание «своих» целей;

- в качестве средств доведения управляющего воздействия до массовых аудиторий используются СМИ, Интернет и другие каналы передачи информации;

- в операциях ИВ широко используется фальсифицированная информация;

- в операциях ИВ не задействуются методы, использующиеся в других формах борьбы, такие как физический вред, запугивание, психотропные вещества и т.д.

Технологии информационных войн «активно и весьма охотно применяют не только страны Запада (прежде всего, США, где термин «информационная война» официально закреплен в боевом уставе Армии США «Психологические операции»), но и международными террористическими организациями и группировками, такими как запрещенные в РФ «Исламское государство», Аль-Кайда»; «ИГ по всему миру ищет, вербует или просто нанимает на работу высококлассных специалистов в области кибервойны и информационного противоборства, которые в информационно-идеологическом поле вполне успешно конкурируют с силами специальных операций стран Запада» [[23]](http://e-notabene.ru/wi/article_21896.html#23).

На практике организация и проведение ИВ обычно предполагает наличие некоторых этапов:

- формулировка целей;

- разработка стратегии;

- разработка плана тактических мероприятий.

При этом ряд ученых считают, что все операции информационной войны, ведущейся на данном этапе российско-американских отношений, укладываются в одну общую организационно-технологическую схему [[23]](http://e-notabene.ru/wi/article_21896.html#23). Эта точка зрения при определенных допущениях имеет право на существование (если сознательно ограничить поле исследования информационных войн только американскими операциями, осуществленными США против Российской Федерации в период с 2014 по конец 2016 года). Но именно эти допущения, носящие принципиальный характер, и ограничивают универсальность данного подхода: так, скандал с так называемым «российским вмешательством» в избирательную кампанию Хиллари Клинтон выходит за рамки данной схемы, приведенной в [[23]](http://e-notabene.ru/wi/article_21896.html#23); недавний скандал с изъятием у российских дипломатов в Нью-Йорке и Вашингтоне служебных дач, вылившийся в «войну санкций», и вовсе не укладывается в данную схему, как, впрочем, и в любую другую. Эти примеры наглядно свидетельствуют о том, что в современных международных отношениях и мировой политике операции информационной войны планируются не шаблонным способом, а ситуативно, с применением множества разнообразных спех, приемов и подходов. Хотя, конечно, нередко используются и «домашние заготовки», апробированные на одном из конфликтов более низкого уровня.

Российские и зарубежные специалисты выделяют семь основных форм информационной войны [[11]](http://e-notabene.ru/wi/article_21896.html#11):

- командно-управленческая;

- разведывательная;

- психологическая;

- «хакерская»;

- экономическая;

- электронная;

- кибервойна.

Однако, несмотря на подобное, довольно подробное, деление на категории, все они взаимосвязаны между собой и обычно в одной и той же информационной войне может использоваться сразу несколько форм информационного противоборства. Самой эффективной и опасной считается психологическая форма действий, поскольку здесь информационная война направлена на большие массы людей в сознание и подсознание которых посредством специальных средств осуществляется внедрение программных и управленческих установок базовой идеологии противника: людям навязывают чуждые им цели и делают это так, что рядовые граждане были уверены, что это именно их собственная, родная идеологическая установка.

Целью любой информационной войны на стратегическом уровне является военное поражение противника, обеспечиваемое информационными средствами, на тактическом – обеспечение добровольного подчинения.

При этом организаторы информационной войны, как правило, решают следующие основные задачи:

- обеспечение собственной безопасности;

- нарушение процесса функционирования системы органов государственной власти и управления противника;

- вербовка граждан;

- нанесение ущерба различным объектам стратегической инфраструктуры государства-противника, а также его национальным интересам;

- навязывание собственных ценностей, интересов и приоритетов;

- подрыв национальной безопасности.

Однако эти задачи в своей предметной и содержательной частях корректируются непосредственно в зависимости от избранных инициатором целей и способов проведения информационной войны. Методами же ведения ИВ являются:

- утаивание важной информации;

- смещение или замена понятий;

- манипулирование общественным сознанием;

- использование «пустой» информации;

- обострение политической борьбы, политическая дестабилизация и инициирование кризисов;

- создание напряженности в общественно-политической атмосфере;

- нанесение ущерба в различных сферах жизни государства и общества.

При этом способами ведения информационных войны выступают аткие известные приемы как «пробные шары», «прайминг», «фрейминг», «наклеивание ярлыков», о которых упоминает [[23]](http://e-notabene.ru/wi/article_21896.html#23).

Что касается объектов информационной войны [[12]](http://e-notabene.ru/wi/article_21896.html#12), то ими могут быть как индивидуальное и массовое сознание, так и информационная инфраструктура, информационные и психологические ресурсы, социально-политические системы и процессы. Особенно мощным информационным атакам подвергаются духовно-нравственная и ценностная сфера, патриотическое сознание и воспитание молодежи, сфера образования.

Субъектами же информационной войны могут выступать [[12]](http://e-notabene.ru/wi/article_21896.html#12):

- государства, их союзы и коалиции;

- международные организации;

- негосударственные незаконные вооруженные формирования и организации террористической, экстремистской, радикальной политической, радикальной религиозной направленности;

- транснациональные корпорации;

- виртуальные социальные сообщества;

- средства массовой информации и массовой коммуникации;

- виртуальные коалиции.

При этом каждый из указанных субъектов в информационной войне преследует свои собственные интересы, лежащие в политической плоскости. В условиях информационной войны ее участники:

- используют технологии манипулирования информацией для осуществления атак класса «панамский вброс» на противника;

- используют военные информационные функции для повышения общей эффективности вооруженных сил (если субъекты ИВ – государства, их союзы и коалиции);

- используют информационные методы воздействия на противника и информационные технологии для обеспечения собственной безопасности.

Если говорить о манипулировании информацией, то это – один из самых распространенных приемов информационного воздействия и внешнего управления, широко использующийся, в том числе, в информационной войне. Так, в последнее время довольно активно используется феномен «кликбейт», наиболее ярко проявляющий себя на видеохостинге «Youtube». Дословно данный термин можно перевести как неявный призыв «нажать на приманку»: такие призывы часто используют рекламщики-маркетологи для завлечения клиентов в интернет-магазины.

Суть действия «кликбейта» такова: используя баннер с каким-либо провокационным контентом, владелец сайта фактически вынуждает посетителя нажать на него («кликнуть»), после чего происходит переход на какой-либо рекламный сайт, либо на сайты с азартными играми; с помощью «кликбейта» также существует возможность занести вирус на свой компьютер. Сегодня «кликбейт» используется практическими всеми СМИ для привлечения читателя, и этот феномен наглядно демонстрирует современные возможности манипулирования информацией в собственных целях.

Существует также ряд определенных правил оформления «кликбейта» [[13]](http://e-notabene.ru/wi/article_21896.html#13). Так, в типичный «кликбейт» входят следующие составляющие: обращение в единственном числе и использование указательных местоимений; нестандартная пунктуация и большое число эпитетов; сокрытие части информации; активное использование цифр и «шокирующих» изображений и т.д. Часто встречаются ситуации, когда заголовок «кликбейта» не соответствует его содержанию, и с помощью этого может осуществляться переключение внимания людей на информационные поводы, несущие прямую угрозу их безопасности или психическому здоровью. В этом случае подобного рода информационные приемы и технологии, попадая в руки экстремистов, киберпреступников или инициаторов информационных войн, становятся угрозой информационной безопасности не только личности и общества, но и государства.

В Доктрине информационной безопасности Российской Федерации [[14]](http://e-notabene.ru/wi/article_21896.html#14) используется следующие определение информационной безопасности: информационная безопасность Российской Федерации – это «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [[14]](http://e-notabene.ru/wi/article_21896.html#14). При этом понятие угрозы информационной безопасности Российской Федерации определяется как «совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере» [[14]](http://e-notabene.ru/wi/article_21896.html#14). Информационные войны всех известных видов, очевидно, полностью подпадают под понятие угроз информационной безопасности РФ, сформулированное в соответствующей Доктрине информационной безопасности Российской Федерации.

Между тем, эффективность операций информационной войны часто зависит не столько от избранных способов и методов информационного воздействия на противника, сколько от ширины и синхронности охвата этим воздействием массовых аудиторий, то есть – от каналов доведения управляющего информационно-психологического воздействия до сознания конкретных граждан. Возникает парадокс: с одной стороны, инициатор информационной войны под избранные им цели или конкретные задачи может разработать весьма тонкие и действенные технологии манипулирования индивидуальным и массовым сознанием; с другой стороны, применение этих технологий на практике может не дать решительно ничего, если каналы доведения воздействия до избранных целевых или массовых аудиторий будут выбраны неправильно или отсутствовать вовсе. В этом плане в современных информационных войнах СМИ и «новые медиа», вопреки мнению многих ученых (например, [[12]](http://e-notabene.ru/wi/article_21896.html#12)), являются не столько независимыми, автономно действующими субъектами конфликта, сколько сетевыми каналами доведения управляющего воздействия до массовых аудиторий, на которые это воздействие рассчитано. Таким образом, при классификации субъектов ИВ следует сократить их количество, ограничившись акторами, действительно способными нанести своему противнику военное поражение методами информационной войны – государствами, их союзами и коалициями, а также обладающими международной правосубъектностью международными межправительственными организациями. Также осторожно следует относиться и к виртуальным субъектам (сообществам, коалициям), поскольку они чаще всего используются в ИВ в качестве средств достижения цели, занимая подчиненное положение по отношению к национальным государствам и их правительствам.

Сегодня многие исследователи информационных войн, стремясь познать природу их происхождения, закономерности эволюции форм и методов, обращаются к событиям сравнительно недавнего прошлого – к периоду «Холодной войны», справедливо считая, что этот конфликт, наряду с военной и экономической составляющей, был еще и информационным. В определенной степени они действительно правы: противостояние СССР и США было, в первую очередь, борьбой двух идей – коммунизма и капитализма – и столкновением двух идеологий. Более того, можно утверждать, «Холодная война» между Россией и США продолжается и сегодня: просто она изменила свою форму и стала, в первую очередь, информационной. Продолжается она и сегодня: на протяжении нескольких лет можно наблюдать активную информационную борьбу США и России, которая выражается в различных «вбросах» [[16]](http://e-notabene.ru/wi/article_21896.html#16) [[18]](http://e-notabene.ru/wi/article_21896.html#18), фальсификации информации в официальных и неофициальных источниках, провокациях граждан страны-противника, создании новых средств по обеспечению собственной безопасности и проникновению в информационную инфраструктуру противника.

К одному из таких средств относится создание канала Russia Today (RT) [[15]](http://e-notabene.ru/wi/article_21896.html#15), который начал свое существование в 2005 году и на сегодняшний момент состоит в пятерке самых просматриваемых каналов США. Помимо этого, он вещает более чем в ста различных стран мира, на различных языках, имеет свои студии в Вашингтоне и Лондоне, где также осуществляется вещание на англоязычные аудитории. На канале работают лучшие специалисты, которые рассказывают о России в других странах и показывают гражданам этих стран, что происходит в мире и как именно выглядит политика их страны со стороны. Таким образом, осуществляется один из способов защиты российской инфраструктуры и национальных интересов Российской Федерации и одновременная дискредитация пропаганды противников и недоброжелателей России. О высокой эффективности деятельности RT и других средств российского иновещания, влияющие на сознание американцев и других жителей Западного мира, неоднократно заявляли официальные лица на Западе, выступавшие с острой критикой «пропаганды Кремля».

Таким образом, резюмируя вышесказанное, можно прийти к заключению о том, что современная информационная война имеет разные формы, среди которых командно-управленческая, разведывательная, психологическая, хакерская, экономическая, электронная и кибервойна. Все они коррелируют между собой и чаще всего используют несколько форм информационной войны для лучшего воздействия на противника.

Из соответствующих целей субъектов информационной войны формируются ее задачи, которые в обобщенном виде представляют собой обеспечение собственной безопасности, нарушение или уничтожение процесса осуществления информационной защиты противника, вербовка граждан, нанесение ущерба различным инфраструктурам страны, а также ее национальным интересам.

Следует также отметить, что информационная война отличается от других типов войн, и главное из ее черт является навязывание противнику «необходимых» мыслей, настроений, формирование ложной идеологии в целом.

При этом СМИ и «новые медиа» действительно широко используются участниками информационной войны для оказания информационного давления на соперника, для дезинформации, манипулирования, дискредитации и формирования позитивного ил негативного образа как самого политического конфликта, принявшего форму ИВ, так и любого из его участников. Участники информационной войны проводят через каналы СМИ информационные кампании, направленные против соперников, осуществляют вбросы и контролируемые утечки информации, развязывают «войны компроматов» и т.д. Блогосфера активно используется для распространения слухов и создания политических мифов, а также для консолидации союзников, разложения противников, внедрения в массовое сознание программных установок на борьбу с кем-либо, для продвижения своей идеологии.

Вместе с тем, современные информационные войны все же не являются смертельной угрозой государству и обществу: в информационных войнах и связанных с ними политических конфликтах побеждает тот, кто умеет предсказать действия своих противников на несколько шагов вперед, просчитать их с высокой степенью точности. Для этого весьма полезными становятся технологические схемы операций и контропераций информационной войны, разрабатываемые российскими учеными на примере американского опыта, с адаптацией к российским условиям [[23]](http://e-notabene.ru/wi/article_21896.html#23).

**Литература:**

1. Толковый словарь Ожегова. С.И. Ожегов, Н.Ю. Шведова. 1949-1992.

2. Политология. Словарь. — РГУ. В.Н. Коновалов. 2010.

3. Восстание масс // Ортега-и-Гассет Х. Восстание масс: Сб.: Пер. с исп. М.: ООО «Издательство АСТ», 2003.

4. Большой юридический словарь. — М.: Проспект. А. В. Малько. 2009.

5. Понятие информационной войны в международном праве / Т. Р. Короткий, Д. А. Коваль // Альманах международного права.-2010.-Выпуск 2.-С. 331-343.

6. Манойло А.В. Государственная информационная политика в особых условиях: Монография. М.: МИФИ, 2003. – С. 246

7. Швец Д.А. Информационное управление как технология обеспечения информационной безопасности, Сб. «Массовая коммуникация и массовое сознание», М., МГИМО, 2003.

8. Что такое информационная война? [Электронный ресурс]. – URL: http://voprosik.net/chto-takoe-informacionnaya-vojna/

9. Слипченко В.И. Войны шестого поколения. Оружие и военное искусство будущего. М.: Вече, 2002, С. 153.

10. Панарин И.Н.: В информационных войнах у России должен быть крепкий щит и острый меч [Электронный ресурс]. – URL: http://www.aif.ru/society/igor\_panarin\_v\_informacionnyh\_voynah\_u\_rossii\_dolzhen\_byt\_krepkiy\_schit\_i\_o

11. Гузев С. А., Комиссарова М. Н. Информационные войны: типы и особенности // Современные наукоемкие технологии. 2013. №10-2.

12. Манойло А.В. Объекты и субъекты информационного противоборства [Электронный ресурс]. – URL: http://psyfactor.org/lib/psywar24.htm

13. Бабкин С.Н. Как вас заставляют кликнуть по заголовку [Электронный ресурс]. – URL: http://www.lookatme.ru/mag/how-to/inspiration-howitworks/211165-clickbait-grammar

14. Доктрина информационной безопасности Российской Федерации [Электронный ресурс]. – URL: https://rg.ru/2019/12/03/doktrina-infobezobasnost-site-dok.html

15. О канале [Электронный ресурс]. – URL: https://russian.rt.com/about

16. Вепринцев В.Б., Манойло А.В., Петренко А.И., Фролов Д.Б. Операции информационно-психологической войны: краткий энциклопедический словарь-справочник. — М., 2005.

17. Расторгуев С.П., Литвиненко М.В. Информационные операции в сети Интернет / Под общ. ред. А.Б. Михайловского. — М.: АНО ЦСОиП, 2014. — 128 с.

18. Манойло А.В. Иран и США: сложная игра с многовариантным результатом. // Национальная безопасность / nota bene. 2012. № 2. С. 88-95.