

Министерство образования и науки Российской Федерации
Федеральное государственное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Институт лингвистики и международных коммуникаций
Кафедра международных отношений и зарубежного регионоведения

РАБОТА ПРОВЕРЕНА

Рецензент, (должность)

_____ (И.О. Ф.)

_____ 2017 г.

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой, к.т.н., доцент

_____ Л.И. Шестакова

_____ 2017 г.

Информационная война как стратегия «мягкой власти» в
современном мире

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ–410305.2017.407.ПЗ ВКР

Руководитель ВКР, д.ф.н., профессор

_____ Е.Г. Прилукова

_____ 2017 г.

Автор проекта

студент группы ЛМ-425

_____ Е.Н. Нархов

_____ 2017 г.

Нормоконтролер, к.и.н., доцент

_____ А.А. Попов

_____ 2017г.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	7
1 ИНФОРМАЦИОННАЯ ВОЙНА: ТЕОРЕТИКО - МЕТОДОЛОГИЧЕСКИЙ АСПЕКТ	11
1.1 «Информационная война»: понятие и основные характеристики	11
1.2 Технологии и специфика ведения информационной войны.....	25
2 ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО В XXI ВЕКЕ НА ПРИМЕРЕ АРАБО-ИЗРАИЛЬСКОГО КОНФЛИКТА.....	34
2.1 Роль «кибервойны» в контексте решения палестинской проблемы	34
2.2 Поиски путей противодействия информационным войнам на Ближнем Востоке, и их потенциал.....	41
ЗАКЛЮЧЕНИЕ.....	53
БИБЛИОГРАФИЧЕСКИЙ СПИСОК.....	56

ВВЕДЕНИЕ

Проблема информационной безопасности приобрела особое значение на рубеже XX-XXI веков с началом эпохи массовой компьютеризации и внедрением информационных технологий во многие сферы общественной жизни. Сегодня страна, стремящаяся быть полноправным членом мировой политики, не имеет возможности существовать без развитых информационно-коммуникационных средств и технологий. Однако, помимо преимуществ, научно-технический прогресс влечет за собой новые угрозы как национальной, так и международной безопасности. Информационное пространство становится все более уязвимым и порождает такой феномен как «информационная война».

Столь высокую значимость феномен «информационной войны» приобрел в силу распространения институтов демократии, а, вследствие, и возросшей зависимости политики от общества.

Большинство конфликтов современности, как правило, приводят к прямым вооруженным противоборствам, однако, одним из основных, и на первый взгляд – безопасным способом выяснения противоречий, является информационное пространство. Услышав слово «война», сразу возникают ассоциации с вооруженным столкновением и насилием. Война – это противостояние политических образований, которое характеризуется наличием военных (боевых) действий. Информационная война, в свою очередь, не подразумевает использования оружия, однако также предполагает борьбу. В последнем случае, борьба происходит путем использования информационных средств и технологий¹.

Актуальность и важность данной темы обусловлена с одной стороны тем, что информационные войны приобретают все большую значимость в политике современности, а с другой – любое государство стремится создать эффективную систему борьбы с информационно-психологическим воздействием на его

¹ Девяткина, А.Г. Информационные войны в современных международных отношениях / А.Г. Девяткина // Актуальные проблемы современных международных отношений. 2014. №3. С. 54-59.

граждан. В данной квалификационной работе показаны те «рычаги» воздействия на массовое сознание, которые часто применяются при освещении различных, в том числе и арабо-израильского конфликта, который мы рассмотрим более подробно. Аудитория воспринимает все события через призму средств массовой информации (СМИ). Особое значение имеет то, что в данной работе рассматриваются Интернет-СМИ, то есть качественно новые издания, совмещающие в себе элементы, используемые, как в печати, так и на телевидении, что позволяет читателю увидеть наиболее полную и красочную картину событий.

Таким образом, Интернет - коммуникации – это такие методы общения, при которых передача информации происходит по каналам Интернет с использованием стандартных протоколов обмена и представления данной информации. Информация может передаваться в различной форме - голос, видео, документы, мгновенные сообщения, файлы¹. По сравнению с другими средствами массовой коммуникации (газеты, журналы, листовки, брошюры и т.д.), информация, находящаяся в глобальной сети, является более доступной (доступ к ней имеет любой человек, подключенный к сети Интернет), регулярно обновляемой, не имеет ограничений по объему, сопровождается большим количеством графической информации (фотографии, видеоролики). Кроме того, сегодня, в связи со стремительным развитием технологий, Интернет-журналистика становится своего рода инструментом для наиболее быстрого решения конкретных политических задач².

Объектом исследования данной выпускной квалификационной работы является особенность проявления информационной войны на примере освещения арабо-израильского конфликта.

Предмет исследования – организация информационной войны, неизбежно возникающей при его освещении.

¹ Бабаева, Ю.Д. Интернет: воздействие на личность / Ю.Д. Бабаева, А.Е. Войскунский, О.В. Смылова. М.: Можайск-Терра, 2000. С. 12.

² Балугев, Д.Г. Роль «новых СМИ» в современных политических процессах / Д.Г. Балугев, А.А. Новоселов. Нижний Новгород, 2012. С. 28.

Целью данного исследования является изучение сущности и особенностей информационных войн современности на основе анализа применения коммуникационных технологий – «оружия», используемого в подобных конфликтах.

Для достижения поставленной цели необходимо решение ряда задач:

- проследить взаимосвязь между такими понятиями как «информационная война» и «мягкая сила» («soft power») посредством изучения материалов, представленных отечественными и зарубежными авторами;
- выявить сущность и особенности «информационной войны», а также технологии и специфику ее организации и ведения;
- дать оценку «кибервойне» в рамках арабо-израильского противостояния;
- раскрыть потенциал международного посредничества в попытках урегулирования палестинской проблемы.

Для решения поставленных задач и достижения цели был использован системный метод, как в нашей собственной работе, так и в трудах авторов, на которых опираемся в ходе выполнения данного исследования. Помимо этого, был применен контент-анализа материалов с двух информационно-аналитических порталов: еврейского Isralife.com и палестинского Palinfo.com.

Хронологические рамки исследования охватывают практически 75 лет мировой истории, начиная с момента выхода первой передачи такой вещательной корпорации как «British Broadcasting Company» (BBC) в 1941 году и до наших дней¹. Данные хронологические рамки выбраны с целью лучшего понимания и осмысления проблемы «информационной безопасности» на современном этапе. Однако стоит подчеркнуть, что особое значение данная проблема приобретает, как было сказано выше, на рубеже XX-XXI веков с началом массовой компьютеризации и становление информатизации общества.

При написании ВКР были использованы труды как отечественных, так и зарубежных исследователей: Г.Г. Почепцов, Е.М. Примаков, Е. Сатановский, С.П.

¹ Панарин, И.Н. Первая мировая информационная война. Развал СССР / И.Н. Панарин. СПб.: Питер, 2010. С. 7.

Расторгуев, Дж. Аркуилла, Дж. Най, М. Кастельс и др. Немаловажное значение в исследовании проблемы информационной безопасности имеют монографии и статьи И.Н. Панарина.

Структура работы отражает логику изложения материала.

1 ИНФОРМАЦИОННАЯ ВОЙНА: ТЕОРЕТИКО - МЕТОДОЛОГИЧЕСКИЙ АСПЕКТ

1.1 «Информационная война»: понятие и основные характеристики

Несмотря на тот факт, что понятие «информация» широко используется в современной литературе и повседневной жизни, единого научного определения не существует. Различные научные дисциплины вводят его по-разному. Так, согласно определению основоположника кибернетики и теории искусственного интеллекта Норберта Винера, информация – это обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему. Другими словами, автор утверждает, что вне человеческого сознания информации не существует¹. Вплоть до начала XXI века был достаточно широко распространен содержательный подход к пониманию феномена «информация». В рамках данного подхода определение звучит следующим образом: информация – это сведения, посредством получения которых снимается неопределенность, существовавшая ранее. Таким образом, информацию стоит рассматривать как факты и сведения, с возможностью дальнейшей трансформации в знания².

Однако в связи с тем, что в бытовой жизни стали преобладать вычислительные средства и технологии, недостатки содержательного (или антропоцентрического) подхода стали очевидными. Во-первых, здесь не учитываются информационные процессы, протекающие в таких средах, как: компьютерные программы, компьютерные сети, системы искусственного интеллекта и т.д. Во-вторых, при таком подходе невозможно объяснить генетических закономерностей в живой природе.

Таким образом, понятие «информация» требовало логического расширения своего смысла. В ходе данного расширения был отражен обмен сведениями, как

¹ Винер, Н. Кибернетика / Н. Винер. М.: Наука, 1968. С. 21.

² Shannon, C. A Mathematical Theory of Communication / C. Shannon // Bell System Technical Journal. 1948. P. 384.

между индивидами, так и между человеком и машиной, либо двумя машинами в силу создания Глобальной сети Интернет.

Подводя итог вышеизложенного материала, можно охарактеризовать основные свойства информации, независимо от того, как ее интерпретирует та или иная дисциплина:

- информация должна быть зафиксирована в какой-либо форме (в печатном виде, в электронном варианте, в памяти человека);
- данная запись должна нести смысл;
- информация должна вызывать реакцию, т.е. ее можно использовать с определенной целью (пропаганда нужных воззрений).

Информация, пожалуй, является одним из ключевых инструментов, участвующих в решении как социально-экономических, так и политических проблем современного общества. Исходя из чего, на первый план не только внутренней, но и внешней политики государств выдвигаются стратегии преодоления геополитических разногласий и отстаивания национального суверенитета посредством масштабного информационного потока. Таким образом, государства с высокоразвитым научно-техническим потенциалом имеют политическое, экономическое и даже военное доминирование.

Социум и информационная среда, представленная совокупностью условий, средств и методов на базе компьютерных систем и технологий, главным образом – телекоммуникационных сетей и информационно-коммуникационных средств сети Интернет, в большинстве современных стран активно взаимосвязаны. Социальная сеть стала неким аналогом транснациональной корпорации, но только в сфере коммуникации. Мониторинг социальных сетей позволяет не только выявлять и прогнозировать, но и придавать нужный импульс изменениям, происходящим в отдельных обществах. Такие методы принято называть «мягкой силой», являющейся наиболее перспективной стратегией современности в вопросах манипулирования человеческим сознанием. Одним из инструментов реформирования сознания выступает информационная война, постепенно превращающаяся в одно из наиболее эффективных средств «мягкой власти».

На сегодняшний день существует бесчисленное множество определений феномена «информационной войны». Выделим некоторые из них. Так, согласно определению Н. И. Панарина, информационная война – это комплексное применение сил и средств информационной и вооруженной борьбы¹. По мнению другого отечественного исследователя, информационная война представляет собой некую коммуникативную технологию по воздействию на информационные системы противника с целью дальнейшего достижения информационного превосходства в интересах национальной политики, одновременно защищая собственную информацию и информационные системы². Второе определение, приведенное Д. А. Швецом, представляется более точным, т.к. оно наиболее полно отражает сущность информационных войн современности, главной целью которых является установление контроля над информационной сферой и методами принятия государственных решений.

Прежде чем переходить к дальнейшему рассмотрению вопроса, следует также сказать, что подразумевается под понятием «мягкая сила» («soft power»).

Сущность данного феномена известна на протяжении многих лет, однако, под другим названием, одним из которых является «культурно-идеологическая гегемония». Фразеологическое оформление в качестве политического инструмента «мягкая сила» получила после публикации в 1990 году книги американского политолога Джозефа Ная под названием: «Призвание к лидерству: меняющаяся природа американской власти»³. В данной работе автор интерпретирует «мягкую силу» как один из наиболее эффективных инструментов продвижения собственных интересов, а также нанесения вреда потенциальному сопернику в контексте информационной войны. В общем плане «мягкая сила» является формой политической власти, в рамках которой желаемые результаты достигаются посредством создания привлекательного образа одной стороны и

¹ Панарин, Н.И. Информационная война и власть / Н.И. Панарин. М.: Мир безопасности, 2016, С. 224.

² Швец, Д.А. Информационное управление как технология обеспечения информационной безопасности / Д.А. Швец. М.: МГИМО, 2003. С. 6.

³ Nye, Joseph S. Soft Power. The Means to Success in World Politics / Joseph S. Nye. New York: Public Affairs, 2004.

целенаправленного подрыва репутации противника. Отличительная черта данного подхода заключается в следующем: победа достигается действиями самого противника или анонимным агентом киберпространства¹.

Согласно концепции Дж. Ная государство способно воздействовать на людей при помощи следующего²:

- культура («от кутюр» (Франция)),
- ценности (американская мечта (США)),
- привлекательный внешнеполитический курс.

Характерная черта «мягкой силы» – независимость от государства, которое, как правило, обладает подобной мощью. «Жесткая мощь» («hard power») подвергнута государственному влиянию в большей степени. В этой связи, государству гораздо сложнее управлять первой и намного проще манипулировать второй. Последствия «мягкой силы» - в отличие от экономических санкций и военных экспансий – предвидеть и планировать гораздо сложнее.

Внешиполитический курс способен как усиливать, так и ослаблять активность методов «soft power». Так, например, военные операции Вооруженных сил США в Ираке, согласно заявлению Дж. Ная, нанесли серьезный удар по престижу американских ценностей. Аналогичным образом были восприняты интервенции СССР в Венгрии (1956 год) и в Чехословакии (1968 год); действия Союза были осуждены даже народами стран «социалистического лагеря».

Научно-исследовательская литература XXI века рассматривает новые проявления психологического воздействия информационно-коммуникационных средств (публицистика, радио, телевидение, Интернет). Информационно - психологические войны велись на протяжении всей истории человечества. Достаточно вспомнить проведение и радио - трансляции футбольных матчей в блокадном Ленинграде, что и является проявлениями психологических атак.

¹ Най, Дж.С. Кибер-война и мир. [Электронный ресурс] // ИноСМИ. URL: <http://www.inosmi.ru/usa/20120417/190643982.html>, Режим доступа: свободный. (Дата обращения: 11.03.2017)

² Най, Дж.С. Гибкая власть. Как добиться успеха в мировой политике / Дж.С. Най. Новосибирск-М.: Фонд социопрогностических исследований «Тренды», 2006. С. 54.

Вместе с появлением Интернет возникли кардинально иные возможности обработки общественного сознания в нужном направлении, в кратчайшие сроки и в больших масштабах. Введение Томасом Рона такого понятия как «информационная война» в научный лексикон середины 70-х годов XX века совпадает с периодом формирования глобальной сети Интернет¹. Информационная война характеризуется числом и эффективностью хакерских атак, количеством как созданных, так и обезвреженных вирусных программ, фальсификацией информационных данных в каналах связи и т.д.

Согласно аналитическому отчету, предоставленному одним из ведущих научно-исследовательских институтов, который имел главной целью анализ использования методов и приемов «мягкой силы» в ряде ведущих стран мира, первостепенное значение имеют такие сферы как: культура, образование, бизнес и дипломатия. По результатам исследования за 2015 г. по частоте использования «мягкой силы» лидирующую позицию занимают США. Кроме Соединенных Штатов в число первых пяти входят: Великобритания, Франция, Германия и Австралия².

Успешность США во многом обусловлена повсеместным распространением американской культуры. Появился стереотип о том, что все нобелевские лауреаты – американцы, т.к. США активно привлекают умы со всего мира. Даже заслуги по созданию Интернет и всего, что с ним связано (напр.: социальные сети), несмотря на их международное происхождение, приписывают к ряду американских достижений.

Так, по мнению Сергея Хелемендика, «soft power» - это не «мягкая сила», а американская технология, посредством которой захватывается власть в чужой стране и передается нужным лицам. Не что иное, как технология переворотов. Однако данная технология является ненасильственной и именно это ее отличает.

¹ Rona, T. P. *Weapon Systems and Information War* / T. P. Rona. Boeing Aerospace Co., Seattle, WA, 1976. P. 7.

² Рейтинг «мягкой силы». *The Soft Power 30* [Электронный ресурс] // Официальный сайт ИМЭМО. URL: http://www.imemo.ru/index.php?page_id=502&id=1773, Режим доступа: свободный. (Дата обращения: 07.03.2017)

«Soft power» имеет своей главной целью долгосрочный, а лучше – постоянный, контроль над собственностью и моментный контроль над властью, позволяющий осуществить перспективные начинания. Такое слово, как «ограбление» звучит в данном случае недипломатично, но точно описывает суть феномена «soft power»¹.

Помимо захвата собственности, с помощью «soft power» достигают результатов стратегического значения. Например, как появляется надобность в военной базе на территории одной из республик Средней Азии, сразу же вдруг начинаются недовольства и всплески борьбы за свободу; нужно взять под контроль транзит нефти и газа – и начинается борьба то на Кавказе, то в Турции или Греции. Влиянию «soft power» подвержены многие – ведь США умеют привлекать массы к борьбе за свои ценности².

При этом Дж. Най утверждает, что реальной угрозы для США в современном обществе XXI века не существует; никто не способен влиять на мнения граждан Америки таким образом, что это будет негативно влиять на независимость и безопасность страны.

Автор концепции «soft power» расширяет сферу влияния своего феномена, указывая на то, что всякому лидеру необходимо сочетать «жесткую силу» (военные и экономические средства давления) и «мягкую силу» (создавать привлекательный имидж государства). По мнению Найа, именно сочетанием таких методов правления и отличаются успешные лидеры.

Автор уверяет, что невозможно лидировать, не обладая при этом силой; «мягкой» или «жесткой» - неизвестно. Лучше всего сочетать эти 2 вида силы, чтобы добиться успеха. Такое сочетание ведет непосредственно к созданию третьего типа силы, который известен как «умная сила», позволяющий решать ранее непреодолимые трудности.

Таким образом, сущность силы, «жесткой» или «мягкой», заключается в возможности (наличие необходимых властных ресурсов) и умении (реализация

¹ Soft Power - мягкая сила «made in USA» [Электронный ресурс] // Персональный сайт Сергея Халемендика. URL: <http://www.chelemendik.ru/ShowDoc.php%3Fd%3D620>, Режим доступа: свободный. (Дата обращения: 18.03.2017)

² Там же.

властных ресурсов) добиваться желаемых результатов от других акторов международных отношений.

Информационные войны, пожалуй, ведет практически каждое государство современности. Однако стоит отметить, что «мягкой силой», способствующей успешному информационному противостоянию, на данный момент развития обладают лишь США. Исторически это «изобретение» приписывают американцам. Оно, конечно, не является таким масштабным как фондовая биржа в Нью-Йорке, но его значение возрастает с каждым годом. «Soft power» как глобально действующая система переворотов, инструмент смены власти по воле США, обязана тысячи специалистам, напряженно работающим в умственном и творческом плане над ее созданием в течение ни одного десятилетия¹.

Стратегия «мягкой силы» воплощает в себе сугубо экономический подход, который понятен любому гражданину, а значит и является эффективным. Исторически сложилось, что цивилизации и отдельные народы старались доминировать, смешивая деньги, традиции, власть, мораль. Данное предубеждение являлось ошибочным².

Существуют основания предполагать, что времена «soft power» уходят в прошлое. Но это не означает, что культурам и народам станет существовать легче. Может быть, появится нечто новое и вовсе не американского толка. Россия пытается создать свою «мягкую силу», проявления которой усиливаются с каждым годом. Желание выстроить эффективную концепцию «мягкой силы» обосновано ее результативностью. Уже заметны некие результаты в рамках постсоветского пространства. Россия всегда отличалась умением выстраивать долговременные союзы с представителями различных народов, населяющих государство.

Процессы глобализации и унификации информационного пространства, произошедшие в конце XX – начале XXI веков в силу повсеместного

¹ Soft Power - мягкая сила «made in USA» [Электронный ресурс] // Персональный сайт Сергея Халемендика. URL: <http://www.chelemendik.ru/ShowDoc.php%3Fd%3D620>, Режим доступа: свободный. (Дата обращения: 18.03.2017)

² Там же.

распространения сети Интернет, повлекли за собой развитие информационно-коммуникационных технологий. Последние, в свою очередь, привели к существенным изменениям в большинстве сфер жизнедеятельности общества.

Информация, в отличие от материальных ресурсов, включая технические, является неисчерпаемым источником. Информация – это результат творческого труда индивидов, следовательно, ее количество, по истечении определенного срока лишь увеличивается, в силу процессов развития и массового потребления. Сегодняшняя динамика роста информационных ресурсов показывает, что их количества возрастает в 2 раза по истечении каждых 20 месяцев, по сравнению с полувековым промежутком времени в эпоху К. Маркса¹.

Под понятием информационно-коммуникационных технологий (ИКТ) зачастую подразумеваются технологии, главной целью которых является накопление, обработка, передача и интерпретация информации в необходимой форме. ИКТ также включают в себя программно-технологические методы, позволяющие воспринимать и пользоваться информацией без видимых затруднений².

Театр действий ИКТ представлен следующими компонентами, а именно: компьютерами, установленным на них программным обеспечением и «всемирной паутиной», связывающей все это. ИКТ подразделяются на следующие группы:

- сберегающие – технологии, основной задачей которых является хранение данных;
- рационализирующие – технологии. Упрощающие поиск информации;
- творческие – технологии, посредством которых человек взаимодействует с информацией.³

В рамках информационной войны наиболее рационально рассмотреть творческие технологии, т.к. именно они способствуют формированию

¹ Абдеев, Р. Ф. Философия информационной цивилизации / Р. Ф. Абдеев. М.: ВЛАДОС, 1994. С. 7.

² Бернейс, Э. Манипуляция общественным мнением: как и почему / Э. Бернейс // Полис: политические исследования. 2012. №4. С. 149.

³ Маринко, Г.И. Управленческий консалтинг / Г.И. маринко. Учеб.пособие. М.: Инфра-М, 2005. С. 63.

личностных суждений человека и способны дезинтегрировать общество, в силу искаженного толкования фактов.

Общество XXI века является информационным и не что иное, как телекоммуникационные средства определяют путь его развития. Телекоммуникационные сети не имеют ни культурных, ни национальных границ. До появления унифицированных сетей связи человеку приходилось преодолевать географическое пространство, для получения информации, либо достижения коммуникации.

Информационные технологии современности – это технологические системы стратегического значения, включающие политический, социальный и культурный аспекты. ИКТ сформировали новую концепцию миропорядка, которая претворила в жизнь, некогда произнесенную Уинстоном Черчиллем фразу: «кто владеет информацией, тот владеет миром». Именно доступ к информации, а не ее количество является фактором социальной дезинтеграции, которая подразумевает распад единого целого на части. Человечество привыкло к информационным реалиям современности, подразумевающим отсутствие необходимости самостоятельного поиска информации; люди стали пассивно потреблять информацию, рассчитанную на массы. В этой связи появляется понятие «одномерного человека»¹. Распространение авторитаризма в политике и культуре объясняется также пассивностью выбора информации, ее дозированной и отказом граждан от участия в общественной жизни страны.

На первый взгляд кажется, что бесчисленное число СМИ, являющихся одним из инструментов ИКТ, формируют индивидуальный характер и сознание человека, предоставляя ему возможность выбора. Однако, подавляющее количество людей смотрит одни и те же телевизионные каналы, программы, подаваемые в определенном формате; читает те же статьи в газетах и журналах; слушает схожие радиостанции и т.д. Данная ситуация вызывает неоднозначное отношение к СМИ. С одной стороны, медиасредства оказывают положительное

¹ Кравченко, С.А. Социология: парадигмы через призму социологического воображения / С.А. Кравченко. Учеб.пособие. М.: Экзамен, 2007. С. 498.

влияние на личностную осведомленность, с другой – манипулируют сознанием масс.

Ярким подтверждением вышесказанного является транслирование мировых событий международной телекомпанией «Аль-Джазира», сферой влияния которой является не только ближневосточный регион. Спустя 5 лет после создания, де-факто, независимого телеканала, «Аль-Джазира», к 2001 году, перехватила инициативу вещания региональных событий у западных компаний, став единственной медиа-корпорацией, ведущей прямую трансляцию событий из Афганистана¹. В сложившейся ситуации, не имея альтернативной точки зрения, мировое сообщество было вынуждено признать телеканал, который имел возможность манипулировать мнением масс, посредством интерпретации фактов.

Сегодня, информационная пропаганда является скорее заботой государственных идеологов и СМИ, нежели предметом рассуждения рядовых граждан. ИКТ оказывают существенное влияние на медийную составляющую современности, превратив медийную отрасль в совершенное средство пропаганды. Появилась возможность «питать» общество тем, что до XXI столетия считалось специальными средствами информационной войны.

По мнению В.А. Рубанова использование средств дезинформации общества в мирное время недопустимо в связи с тем, что мероприятия пропагандистского толка затрагивают не отдельного противника, а все общество в целом. В первую очередь страдает сама информация, ведь весь ее смысл состоит в достоверности. Далее происходит социальная дезинтеграция среди групп, придерживающихся различных точек зрения, которая влечет за собой информационную войну, нередко переходящую в открытые вооруженные столкновения².

Специфика современных конфликтов заключается в том, что информация уже не есть некий дополнительный ресурс. В настоящее время информацию можно, и

¹ Варганова, Е.Л. Медиа-экономика в информационном обществе / Е.Л. Варганова. М.: Информационное общество, 2011. С. 12.

² Информационная война и цифровой мир [Электронный ресурс] // Сайт Независимой газеты. URL: http://www.ng.ru/stsenarii/2016-04-26/12_infowar.html, Режим доступа: свободный. (Дата обращения: 23.03.2017)

даже нужно, рассматривать как самостоятельный и очень важный ресурс, который во многих конфликтах имеет решающее значение. Помимо прочего, это отразилось в появлении термина «информационная война».

В XXI веке информационные войны стали одним из самых распространенных видов конфликтов, по эффективности не уступая обычным (традиционным) войнам¹.

Более того, понятие информационной войны по своей сути шире традиционного понимания войны как открытого противостояния между враждебными силами. В современном мире информационные войны могут проходить (причем, весьма ожесточенно) и при сохранении формального мира как внутри страны, так и на международной арене. Классическим примером первого является практически любая избирательная кампания, примером второго случая – информационная война, развязанная западными странами против России в связи с украинскими событиями 2014 года.

Как и всякая война, информационное противостояние имеет свои жертвы (причем не только «информационные») и свою специфику проведения. В этом смысле в XXI веке информационные войны развиваются весьма бурно в следующих направлениях²:

- техническая составляющая все более подчиняется гуманитарной составляющей;
- гуманитарная составляющая доходит до уровня когнитивного измерения, что, помимо прочего, изменяет цели атак в информационном противостоянии;
- значительное усиление электронной составляющей информационного противостояния, что приводит к ускоренному развитию такого явления как «кибервойны».

¹ Брусницын, Н.А. Информационная война и безопасность / Н.А. Брусницын. М.: Вита-Пресс, 2001. С. 67.

² Там же.

Известный исследователь данной проблематики Дж. Аркилла считает, что специфика ведения информационной войны все больше определяется следующими факторами¹:

- информационная сфера все в большей степени воспринимается как средство борьбы и все больше взаимодействует с традиционной военной составляющей конфликтов (войн);
- различного рода сетевые организации становятся важнейшим фактором в конфликтах;
- самые разные информационные операции все более четко проявляют свою мультимедийную суть.

Возрастание роли информационной составляющей на международной арене связано с целым рядом факторов, среди которых следует отметить следующие²:

- все больше стран в мире вступают в стадию развития, которая определяется как информационное общество, причем этому не препятствует даже слабый уровень развития экономики и сохранение традиционного менталитета (в некоторых ситуациях он, напротив, оказывается весьма подходящим для проведения информационных операций);
- в большинстве случаев военные проекты финансируются лучше, нежели гражданские, что привлекает квалифицированных специалистов в области информационного противоборства;
- перенос средств информационного противостояния во внешнюю политику облегчается тем, что они уже достаточно опробированы применением внутри страны.

Появившись как определенное дополнение к политическим и военным акциям, дополнение, которое использовало многие средства названных сфер, в настоящее время информационная война, став вполне самостоятельным явлением, способна формировать и формирует собственные средства достижения результата.

¹ Arquilla, J. Looking ahead: preparing for information-age conflict / J.Arquilla, D. Ronfeldt. Athena's camp. Santa Monica, 1997. P. 11.

² Жуков, В. Взгляды США на ведение информационной войны / В. Жуков // Зарубежное военное обозрение. 2001. №1. С. 57.

Общепризнано, что информационная сфера обладает собственной спецификой, не сводимой к специфике других сфер, что делает оправданным разработку и совершенствование собственных средств противостояния.

Так, все большее значение приобретает этический аспект действий, но не по причине высокой нравственности бойцов информационного фронта, а потому, что в рамках демократических, да и не только, обществ весьма важным становится поддержка противостояния, которая невозможна, если противостояние воспринимается как несправедливое. Так, не в последнюю очередь в свое время Франция потеряла Алжир по причине того, что население страны воспринимало войну в этой колонии как несправедливую. Именно поэтому, как и во времена Платона, уделяется значительное внимание проблеме справедливости, нахождению средств обоснования справедливости тех или иных действий¹. Достаточно указать на обоснование странами Запада вторжения в Югославию и Ирак: различного рода рассуждения о справедливости занимали в этом обосновании далеко не последнее место.

Специфика ведения информационной войны сегодня предполагает использование следующих технических способов:

- различного рода компьютерные вирусы, способные размножаться, внедряться в программы, передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и т.д.²;

- так называемые «логические бомбы», под которыми понимают программные устройства, которые заранее внедряются в информационно-управляющие центры военной или гражданской инфраструктуры, чтобы по сигналу или в установленное время привести их в действие;

- разнообразные средства подавления информационного обмена в телекоммуникационных сетях, фальсификации информации в каналах государственного и военного управления;

¹ Гриняев, С. Концепция ведения информационной войны в некоторых странах мира / С. Гриняев // Зарубежное военное обозрение. 2002. №2. С. 13.

² Там же. С. 15.

- специальные средства для нейтрализации тестовых программ;
- всевозможные ошибки, которые специально вводятся в программное обеспечение объекта, искажая или делая невозможным его нормальную деятельность¹.

Однако, как уже отмечалось, техническая составляющая информационных противостояний в настоящее время не является главной. Более важны гуманитарные аспекты, поскольку современные информационные операции предполагают изменение картины мира в целом больших групп населения (чаще всего – целых государств), а не просто внедрение тех или иных сиюминутных представлений. Это приводит к тому, что информационная среда рассматривается как комплексная система, от которой зависит успех военных операций². Такого рода информационное противостояние является сравнительно новым явлением, аналоги которого немногочисленны: специалисты в качестве такового указывают чаще всего на холодную войну между СССР и США³.

Одним из способов ведения такого рода новых информационных войн специалисты считают открытие закрытых обществ. Подобного рода действия предполагают либерализацию, подвергающуюся воздействию страны изнутри, формально – посредством внутренних сил, которые, на самом деле, руководствуются инструкциями извне. Это своеобразный информационный вариант «пятой колонны».

При таком подходе информация выполняет следующие важные функции:

- способствует сравнительно быстрому изменению традиционных сфер (экономической, политической, военной);
- приводит к возникновению специально разрабатываемой информационной стратегии;
- установка на открытость сменяется на установку охраняемой открытости.

¹ Шкрабков, В.Н. Информационное оружие и информационные войны / В.Н. Шкрабков. М.: Сориум, 2001. С. 91.

² Там же.

³ Там же. С. 92.

В большинстве случаев информационная атака, в отличие от традиционной войны, происходит незаметно для того, кто ей подвергается. Конечно, имея определенные знания, ее можно заметить, но большинство населения такими знаниями не обладает и вряд ли будет обладать в силу своей недостаточной интеллектуальной развитости (по причине того, что это им не нужно в повседневной жизни, так же, как им не нужна тригонометрия, которую население в своей массе также не знает, хотя и изучает в школе).

Не требуя существенных затрат (в сравнении с традиционной войной) со стороны атакующего, информационная атака может легко превращаться (и чаще всего превращается) в непрерывную¹.

Более того, если обычная атака не способна быть долгое время интенсивной в силу различных объективных факторов, связанных с физическими ограничениями, то информационная атака может непрерывно увеличивать свою интенсивность, легко достигая порогового для человека уровня, после которого деструкция его основных жизненных сил становится необратимой².

Таким образом, информационное противоборство представляет собой масштабные (в рамках определенного района страны, всего государства или региона) и оперативные действия, направленные на достижение информационно-психологического превосходства над противником, посредством вброса нужных воззрений.

Для более полного понимания сущности информационной войны следует более подробно рассмотреть ее технологии и специфику ведения.

1.2 Технологии и специфика ведения информационной войны

Ранее мы определили понятие «информационной войны» и дали ее основные характеристики, теперь рассмотрим ее ведение. Информационное воздействие не

¹ Манойло, А.В. Государственная информационная политика в особых условиях / А.В. Манойло. Монография М.: МИФИ, 2003. С. 42.

² Там же.

изменяет непосредственно физического состояния людей (хотя опосредованно способно и на это), оно изменяет сознание человека, которое формирует реальность, в которой он живет. Поэтому, изменяя сознания, можно добиться не только «идеальных», но и вполне материальных результатов, сделать даже так, что человек будет действовать во вред самому себе. Видимое отсутствие разрушений и трупов во время информационной войны облегчает такого рода действия, поскольку у человека долгое время (нередко – до самого конца) не возникает чувства опасности и желания защищаться, отстаивать собственные интересы.

Перманентность информационной войны все больше превращает ее в новом тысячелетии в атрибут повседневности. При этом она ведется как внутри страны, так и за ее пределами. При помощи искаженной или неполной информации подрываются репутации, выдвигаются обвинения, открываются судебные дела, банкротятся предприятия, осуществляются политические отставки, гонения и т.д. Практически нет такой цели, которая не могла бы быть достигнута при помощи современной информационной войны¹.

Развитие современных информационных технологий, а также средств и методов ведения информационной войны увеличивает ее возможности и незащищенность, как отдельного человека, так и общества в целом от несанкционированного вредоносного воздействия².

Сложность ситуации определяется тем, что развитие различного рода информационных технологий имеет множество позитивных сторон, улучшает человеческую жизнь, способствует развитию экономики. Другими словами, не стоит дегуманизировать информационные технологии и информационное общество в целом, не стоит представлять его как некое абсолютное зло. Речь должна идти лишь о том, что как и всякая технология, информационные технологии имеют и обратную сторону, могут использоваться во вред человеку и

¹ Кастельс, М. Информационная эпоха: экономика, общество и культура / М. Кастельс. Пер. с англ. под науч. ред. О. И. Шкаратана. М.: ГУ ВШЭ, 2000. С. 411.

² Там же. С. 412.

обществу. Для того, чтобы эффективно противостоять этому негативному аспекту развития информационных технологий, необходимо укреплять как традиционные нравственные ценности, так и разоблачать современные методы информационной войны.

Проблема здесь, однако, заключается в том, что власть не заинтересована в такого рода разоблачениях, поскольку не только является объектом информационного воздействия, но и сама использует подобные методы, применительно к населению. Например - в ходе предвыборных компаний¹.

Конкретизируя, можно указать целый перечень факторов, которые облегчают ведение информационной войны² и, соответственно, устранение которых затрудняет противнику проведение эффективных информационных атак:

- острые (открытые) межконфессиональные и межнациональные конфликты;
- наличие внутри страны групп, которые придерживаются экстремистских взглядов;
- наличие террористических организаций;
- наличие сепаратистских настроений, особенно по национальному признаку;
- наличие острого идеологического противостояния между политическими силами внутри страны;
- высокий уровень преступности, особенно организованной;
- коррупция.

Таким образом, если ранее информационное воздействие было направлено на избранные группы населения, прежде всего на руководство страны, то в новом тысячелетии ситуация изменилась. Теперь информационное воздействие направлено на все население страны с целью изменения его сознания, причем, желательно, долговременное – изменение его картины мира. В этой связи особое внимание уделяется молодежи, поскольку она в силу возрастных особенностей легче поддается воздействию такого рода.

¹ Почепцов, Г.Г. Информационные войны / Г.Г. Почепцов. М.: Рефл-бук, 2001. С. 134.

² Там же.

Целью такого рода воздействия является создание атмосферы бездуховности и безнравственности, манипулирование не только общественным сознанием, но и политическими симпатиями и предпочтениями граждан, что приводит к дестабилизации всей системы общественных отношений, общественной конфронтации, противостоянию власти и граждан, обострению конфликтов разного уровня и типа, продуцированию ошибочных управленческих решений, массовых беспорядков¹.

Отличительная особенность информационного противостояния заключается в наличии явной пропагандистской составляющей, присущей большинству материалов, опубликованным как в Сети, так и демонстрируемым по телевидению, радио, или же – опубликованным в СМИ. Пропаганда - неотделимая часть материалов, которые связаны с освещением конфликта.

Четкого определения понятия «пропаганда» не существует. Так, согласно М.Погорельскому, «пропаганда - редакционная политика государственных и ведомственных СМИ»².

Ф. Джефкинс и Д. Ядин в своей книге «Public Relations» трактуют данное понятие иным образом. Согласно их определению, пропаганда – информация, главной целью которой является поддержка какой-либо точки зрения, интереса или убеждения³.

Ещё одно определение понятия пропаганды дается в монографии М. И. Скуленко «Журналистика и пропаганда». Скуленко сопоставляет понятие «пропаганда» с наиболее близким, по его мнению, понятием «агитация». Сама же пропаганда, как считает автор, представляет собой распространение и утверждение в массовом сознании идеологически обусловленных

¹ Маничев, С.А. Мифология в политических технологиях / С.А. Маничев // Общество и политика: Современные исследования, поиск концепций. Под ред. В. Ю. Большакова. СПб.: СПбГУ, 2004. С. 169.

² Погорельский, М. Современная военная журналистика: опыт, проблемы, перспективы / М. Погорельский, И. Сафранчук. М.: Гендальф, 2002. С. 124.

³ Jefkins, F. Public relations / F.Jefkins, D.Jadin. New York, 2009. P.14.

систематизированных взглядов и представлений, составляющих мировоззренческие позиции личности и общества в целом¹.

Определив, что включает в себя понятие «пропаганда» можно говорить о том, какие цели с её помощью преследуются. В большинстве случаев у обеих противоборствующих сторон цели, с которыми применяется пропаганда, общие. Основная задача пропаганды - мобилизовать и направить ненависть против врага. Пропаганда может стать неплохим и довольно действенным способом развить дружбу с союзниками. Также пропаганду можно успешно использовать как средство влияния на потенциальных союзников, тем самым, способствуя оказанию с их стороны помощи и поддержки. Не исключено и то, что пропаганда может стать своего рода веским доводом, причиной для перехода сочувствующих из стана врагов. И, наконец, пропаганда помогает убедить свой народ в правильности и необходимости происходящего, а также поддерживает дух сражающихся.

Сегодня принято выделять три вида пропаганды: «черная», «белая» и «серая». Если говорить о пропаганде применимо к арабо-израильскому конфликту, то очевидно, что любая из сторон активно использует все три названных типа. Но тезисы, формирующие позиции каждой из сторон, участвующих в информационной войне, различны.

Если говорить об Израиле, то здесь среди основных тезисов можно выделить следующие:

- Ислам - религия, нетерпимая к иноверам, а мусульмане - наиболее подверженная экстремизму группа населения;
- едва ли не каждый араб - террорист, у каждого палестинца за пазухой бомба, а Ясир Арафат – бандит;
- на протяжении тысячелетий арабы подвергались незаконным и несправедливым гонениям. Еврейская нация пережила холокост - геноцид. Арабы

¹ Скуленко, М.И. Журналистика и пропаганда / М.И. Скуленко. Киев, 1987. С. 16.

же были на стороне фашистов, а потому у европейцев есть своего рода моральный долг перед евреями;

- необходимо объединить усилия в борьбе с исламским терроризмом, так называемой «общей опасностью»;

- активное использование тезиса о нелегитимности Палестинской автономии (ПНА) в целом, палестинского руководства в частности.

Подобную позицию можно объяснить с точки зрения психологии израильтян. Она имеет свои особенности. Израильтяне - люди, которые прекрасно понимают, что кроме как на вооруженную силу в их регионе надеяться не на что, а потому охотно служат в армии. Вместе с тем у израильтян присутствует некий «комплекс осажденного народа» - результат постоянного нахождения во враждебном окружении. Большинство политических проблем израильтяне рассматривают, прежде всего, с точки зрения собственной безопасности. И если они чувствуют какую бы то ни было угрозу, то сделают все для того, чтобы ликвидировать источник опасности - это для израильтян не более чем самооборона и меры по поддержанию государственности.

Что касается, Палестины, то тут позиции сводятся к следующему:

- палестинский народ - изгои на своей земле, а в других странах - нежелательные иммигранты;

- Палестина - независимое государство, а Израиль проводит по отношению к нему агрессию;

- те, кого израильтяне называют террористами, у них зовутся шахидами, а теракты носят название «самоубийственных акций»;

- А. Шарон - экстремист, сорвавший «мирный процесс» своим посещением мечети «Аль-Акса» в восточном Иерусалиме. Этот визит спровоцировал первую интифаду;

- на международных конференциях и форумах палестинцы выдвигают тезис о приравнивании политики Израиля к расизму. Апеллируя к антиамериканским и

антизападным настроениям, царящим в Азии и Африке, палестинцы называют политику Израиля и патронирующих ему США «неоколониализмом».

Общее у обеих сторон только то, что и те, и другие оперируют такими понятиями как «народ-изгой», «они - террористы и бандиты» и «их государство - незаконное образование». Но израильтяне настаивают на антиисламских тезисах, а палестинцы - на расизме оппонентов.

Но стоит отметить, что обвинения палестинского руководства в лицемерии со стороны израильтян не беспочвенны. Так, например, в том же 1988 году Я.Арафат в своем обращении к израильтянам на сорок третьей сессии Генеральной Ассамблеи ООН заявил: «Давайте примиримся. Давайте отбросим страх и запугивание. Давайте оставим позади войны, непрерывно бушевавшие в горниле этого конфликта в последние сорок лет. Давайте отбросим все угрозы войн в будущем, жертвами которых могут стать наши и ваши дети»¹.

Но уже в январе 1990 г. Арафат противоречит сам себе, заявляя: «Государство Израиль - порождение второй мировой войны и оно должно исчезнуть, как исчезла Берлинская стена»².

Очевидно, что подобная позиция никоим образом не способствовала мирному процессу, более того, её можно назвать крупной политической ошибкой. Известно, что Я.Арафат не имел полномочий объявлять джихад, ведь он был светским деятелем. И тем не менее в конце октября 1996 г., в лагере беженцев Дегейша он заявил: «Мы знаем только одно слово: Джихад, джихад, джихад!»³.

Столь сильная и серьёзная пропаганда, действовавшая на протяжении десяти лет, не могла не повлиять на сознание палестинцев самым, что ни на есть пагубным образом. Призывы к насилию не способствуют решению палестинской проблемы, но все же случаев, когда люди поддаются этим призывам - множество. Вот, например, слова младшего брата одного из палестинских шахидов, Абдуллы Сохара: «Я готов продолжить дело моего старшего брата, пожертвовав

¹ Бовин, А. 5 лет среди евреев и мидовцев. / А. Бовин М.: Захаров, 2002. С. 49.

² Там же. С. 49.

³ Там же. С. 52.

собственной жизнью, чтобы убить как можно больше евреев. Дело моего брата - праведное. Дайте мне сейчас сумку с взрывчаткой, я тут же пойду убивать израильтян. А еще лучше - израильских солдат. В раю нет блокпостов, нет страдания и боли...»¹.

В этой цитате отчетливо прослеживается одно из главных отличий израильской пропаганды от палестинской. Первая, в отличие от второй, имеет четко выраженную этнорелигиозную окраску. Израильское государство не вполне гражданское общество: там нет своей Конституции - её заменяют одиннадцать основных законов, но среди них нет ни одного, который бы утверждал права человека и гражданина. Сама идея «государства евреев и для евреев» (её разделяет большинство израильтян и евреев диаспоры) - благотворная почва для обвинения в расизме.

Если основываться на тех законах, которые действуют в Израиле, то можно считать, что все граждане этой страны - равноправны. А ведь, не смотря на яростные споры внутри израильского общества, в нем существует своеобразная «шкала ценности граждан»: «первый сорт» - евреи, особенно религиозные, ну а «второй» - все остальные².

Очевидно, что согласно этой «шкале», арабы, мусульмане, христиане, а во многом и неверующие евреи явно относятся к гражданам второго сорта. Вообще, если говорить об арабах, то ненависть к ним насаждалась в Израиле на протяжении десятков лет: Организация Освобождения Палестины (ООП) изображалась как союз террористов, а уж хуже Арафата и вовсе никого не было³.

В декабре 1995 г. религиозная партия Еврейский Дом обвинила правительство Израиля за неспособность справиться с акциями палестинских смертников. В заявлении партийного руководства говорилось: «Вы, господин Рабин, поставили нашу страну на колени. Перед кем? Перед бандой убийц, жаждущих нашего истребления. Мы в нашей вооруженной стране уподобляемся тем несчастным

¹ Бовин, А. 5 лет среди евреев и мидовцев. / А. Бовн М.: Захаров, 2002. С. 70.

² Там же. С. 59.

³ Там же. С. 90.

безоружным евреям, которые в годы Второй мировой войны безропотно шли в газовые камеры»¹.

Подобной пропагандой отравлено целое поколение израильтян. На форуме Центрального еврейского ресурса можно найти раздел, озаглавленный «Ислам и террор» или «Арабские СМИ ведут джихад против Израиля». В обсуждениях на подобных форумах фразы вроде «я не знаю ничего хорошего про этих исламофашистов» или «человекоподобные зверьки мусульмане»².

На сегодняшний день, главный результат информационной войны между Палестиной и Израилем заключается в создании стойкой ненависти между рядовыми гражданами этих государств, дезинтеграции арабо-израильского общества, а также формирование устойчивого образа врага всевозможными способами пропаганды «нужных» воззрений. Причем сила последних такова, что даже если конфликт будет урегулирован в ближайшее время, на избавление от этих стереотипов потребуются долгие годы напряженной работы.

¹ Бовин, А. 5 лет среди евреев и мидовцев. / А. Бовин М.: Захаров, 2002. С. 60.

² Арабские СМИ ведут джихад против Израиля [Электронный ресурс] // Центральный Еврейский Ресурс. URL: <http://forum.sem40.ru/>, Режим доступа: свободный. (Дата обращения: 07.04.2017)

2 ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО В XXI ВЕКЕ НА ПРИМЕРЕ АРАБО-ИЗРАИЛЬСКОГО КОНФЛИКТА

2.1 Роль «кибервойны» в контексте решения палестинской проблемы

В силу развития информационных технологий современности, можно сделать вывод о том, что одним из предпочтительных способов борьбы стала «война» в рамках виртуального пространства. Однако, как преувеличивать эффективность информационных методов борьбы, так и не признать того факта, что «оружие» подобного рода имеет огромный потенциал, не имеет смысла.

Информационное Интернет-противостояние в рамках арабо-израильского конфликта можно разделить на две составляющих. Первую из которых принято называть вновь появившимся термином – «кибервойна», вторая представлена пропагандистской деятельностью на различных информационных порталах глобальной сети Интернет. Прежде чем подробно разбирать эти явления, стоит дать определения понятию «кибервойна».

В научно-исследовательской литературе общепринятого понятия данного термина не существует. Зачастую под «кибервойной» понимается применение вредоносного программного обеспечения с целью нарушения работы информационных систем противника¹.

Кибервойна в контексте арабо-израильского конфликта довольно своеобразна и характеризуется следующим²:

- периодические «вылазки» одной из сторон, так называемая «проба сил»;
- потенциал человеческих ресурсов для ведения Интернет-войны огромен. Как в Израиле, так и в Палестине есть тысячи технически образованных молодых людей, имеющих персональный компьютер с выходом в Интернет.

¹ Портрет настоящей кибервойны [Электронный ресурс] // Information Security со ссылкой на inosmi.ru. URL: http://www.itsec.ru/newstext.php?news_id=60110, Режим доступа: свободный. (Дата обращения: 19.03.2017)

² Более 1,3 млн. подключенных к интернету компьютеров в Израиле, т.е. больше чем во всех арабских странах вместе взятых [Электронный ресурс] // Компьюлента. Режим доступа: свободный. (Дата обращения: 23.03.2017)

Террористы, как правило, поддерживают связь любыми способами. Так, например, Израиль уверен в том, что Усама Бен Ладен в качестве хранилищ для карт объектов инфраструктуры и инструкций для их диверсий использовал порнографические сайты¹. Платные абоненты, которыми также мог стать не каждый, входили на подобный Интернет-ресурс с помощью определенного шифра. Таким образом, информация была закрыта для публичного просмотра. В то же время террорист, имевший доступ к сайту, попав на него, получал всю необходимую информацию для предстоящей операции.

При использовании подобных технологий, просчеты, связанные с обнаружением террористической группы при транспортировке информационных носителей любого рода, например – дисков через границу, сводятся к нулю.

Помимо всего прочего, Интернет – это отличная площадка для вербовки новых воинов. Нередко в Сети можно встретить объявления следующего характера: «Если Вы настоящий исламист, имеете компьютер и хотите бороться с неверными посредством Джихада, но не можете осуществить все это в силу отсутствия самолета или бомбы? Если Вы «лянетесь применять свой талант для уничтожения евреев?» Тогда именно Вы являетесь тем человеком, в котором нуждается «Арабский Электронный Джихад» (АЕИТ)». Данная организация недавно объявила о себе, как о вновь созданной террористической организации, главной целью которой является уничтожение произраильских, проамериканских, а также всех других, неугодных ей, Web-сайтов².

Первая Интифада 2000 года сопровождалась большим количеством хакерских атак как государственных, так и коммерческих сайтов Израиля. Как показывает практика, от подобных действий в первую очередь страдают компании, чья деятельность непосредственно связана с высокими технологиями и электронными операциями; помимо этого хакерским атакам подвержены

¹ Зачем Усаме порносайт? [Электронный ресурс] // Центриальный Еврейский Ресурс. URL: www.sem40.ru, Режим доступа: свободный. (Дата обращения: 24.03.2017)

² Электронный джихад [Электронный ресурс] // Новости от Новикова со ссылкой на nationalreview.com. URL: <http://content.mail.ru/arch/8016/156566.html>, Режим доступа: свободный. (Дата обращения: 24.03.2017)

телекоммуникационные системы, СМИ и учреждения государственной важности. Среди израильских Интернет-сайтов, которые были подвержены атакам со стороны палестинских хакеров оказались: сайт Министерства обороны и Министерства иностранных дел.

Период 2001-2002 годов характеризуется новой волной арабо-израильского противостояния. В эти годы было замечено более 160 хакерских атак израильских информационных порталов. В ответ на что, Израиль взломал около 50 стратегически важных сайтов палестинской стороны среди которых: сайт организации «Хезболла», сайт министерства сельского хозяйства Ирана, а также сайты многих ливанских и иорданских компаний¹. Реакцией со стороны Ливана на действия Израиля, а именно: размещение флага Израиля и гимна на главной странице официального сайта «Хезболла» стали неоднократные призывы арабских пользователей сети-Интернет к «электронному джихаду»². Результатом данной «виртуальной интифады» стали серьезные перебои в работе израильских провайдеров. Но и сионистские хакеры не отступали; они на регулярной основе запускали вирусы на русскоязычные сайты экстремистской направленности. Таким же образом поступали с подобными Web-сайтами на арабском и английском языках³.

Арабо-израильский конфликт в течение полувека пытались разрешить стандартными средствами войны - самолетами и танками. Однако открылся иной фронт - киберпространство. Как говорит Ким Гхаттас из MSNBC: представители Израиля и Палестины ведут ожесточенную виртуальную битву, неустанно

¹ Электронный джихад. Как сражаются палестинские и израильские хакеры [Электронный ресурс] //Деловая пресса» со ссылкой на «Московские новости». URL: http://www.businesspress.ru/newspaper/article_mId_1081_aId_45149.html, Режим доступа: свободный. (Дата обращения: 24.03.2017)

² Израиль и электронный джихад [Электронный ресурс] // Правда.Ru. URL: <http://www.pravda.ru/article/803616.html>, Режим доступа: свободный. (Дата обращения: 24.03.2017)

³ Когда начнется вторая арабо-израильская «кибер-война»? [Электронный ресурс] // Lenta.co.il со ссылкой на Israland Новости. URL: <http://www.lenta.co.il/page/230501hack>, Режим доступа: свободный. (Дата обращения: 25.03.2017)

обрушивая поток дезинтегрирующей информации друг на друга, путем нажатия на гашетку нового оружия информационной эры - клавишу мыши¹.

Так, в конце 2000 года армейские подразделения Израиля по компьютерной безопасности, вместе с американским Центром ФБР по защите национальной инфраструктуры, были подняты по боевой тревоге. Бен Вензке, являвшийся директором «i-Defense», американской фирмы компьютерной безопасности, сравнивал в тот момент кибер-интифаду с войной в Афганистане: «Там тоже появление новой технологии (противовоздушных ракет «Стингер») привело в результате к глобализации исламского терроризма»².

Вензке рассказал и о пропалестинском хакере под псевдонимом «Dodi», который угрожал ему лично. Хакер прислал вирус, известный как «перчатка», смысл которого заключается в уничтожении всех данных на электронном носителе по определенной команде, которой может служить обычное сообщение на электронную почту. Спустя некоторое время «Dodi» угрожал основным американским провайдерам, обещал их разорить; и его угрозы были вполне обоснованными: подобные вирусы уже на тот момент могли быть внедрены в не о чем не подозревавшие об этом компьютерные сети и просто дожидаться команды. Однако, более всего, израильские армейские подразделения по компьютерной безопасности опасались внедрения компьютерных вирусов «массового поражения»³.

«Кибервойна» между Палестиной и Израилем в начале 2000 годов стала ярким примером того, что ущерб в виртуальном пространстве, сегодня, не уступает урону, нанесенному посредством стандартных средств ведения войны. Как сообщает Associated Press: «стороны намерены добиться общественного резонанса; израильские сайты публикуют точку зрения официальных лиц на конфликт. Поэтому, когда официальный сайт пострадал от атаки типа «отказ от

¹ Дисабатино, Дж. Кибервойна на Ближнем Востоке / Дж. Дисабатино // Computerworld Россия. 2000. №42. С. 14

² Радышевский, Д. Электронный джихад / Д. Радышевский // Московские новости. 2002. №4. С. 23.

³ Там же. С. 24.

обслуживания», Израиль утратил одну из возможностей донести до общественности свою позицию»¹.

Взлом официального сайта Кнессета - израильского парламента стал новым этапом кибервойны. Согласно данным Associated Press злоумышленники, как ни странно, изменили лишь пару файлов. Официальное руководство Израиля же этот «проступок» не признает, в силу быстрого урегулирования ситуации. Позже, ответственность за содеянное взяла на себя группа израильских подростков. Одаренные молодые люди заявили, что помимо взлома сайта парламента им также удалось сломать сайт движения «Хезболла». На первый взгляд, казалось, что все только на руку Израилю, если бы не тот факт, что радикальные исламистские сайты распространили информацию, призывая всех своих посетителей атаковать официальные сайты Израиля².

Спустя некоторое время, в январе 2001 года, группа неизвестных хакеров взломала персональный сайт лидера партии «Ликуд» - Ариэля Шарона. После чего на главной странице Web-сайта появляются слова одобрения и поддержки палестинцев и разделяющей их интересы, террористической организации «Хезболла». Помимо этого, по заявлению информационного портала Annova.com хакеры заполучили базу данных избирателей³.

В ответ на произошедшее поступила реплика от руководителя информационного бюро МИД Израиля – Ори Нойя, который подчеркнул, что взламывать сайты - все равно, что сжигать книги. Все это, является весьма символическим деянием, сравнимо со временами нацизма⁴.

В свете неоднократных хакерских атак группой сотрудников ряда израильских IT-компаний была создана организация под названием «Израильское Интернет-

¹ Дисабатино, Дж. Кибервойна на Ближнем Востоке / Дж. Дисабатино // Computerworld Россия. 2000. №42. С. 15

² Там же.

³ Хакеры взломали сайт Шарона и украли базу данных [Электронный ресурс] // Lenta.ru. URL: <http://lenta.ru/internet/2001/01/31/sharon/>, Режим доступа: свободный. (Дата обращения: 27.03.2017)

⁴ Кибервойна на Ближнем Востоке. Противостояние между израильянами и палестинцами переместилось в Сеть [Электронный ресурс] // ComputerWorld. URL: <http://www.osp.ru/cw/2000/42/7800/>, Режим доступа: свободный. (Дата обращения: 28.03.2017)

подполье» (Israeli Internet Underground - ИИ) с главной целью - предотвращение всевозможных кибер-атак информационных ресурсов Израиля¹.

Одним из первых достижений ИИ стал проект «SODA» (от «sod» (иврит) – секрет) разработанный совместно с американской компанией по информационной безопасности 2XS, направленный на «информирование общественности и предложение решений по борьбе с кибервандализмом».

На сайте «Израильского Интернет-подполья» ведется учет взломанных, выведенных из строя, либо «изуродованных» в той или иной степени информационных ресурсов, пострадавших от рук пропалестински настроенных хакеров. На сегодняшний день насчитывается более 40 израильских сайтов государственной важности, которые были подвергнуты влиянию «извне»².

В числе сегодняшних противников ИИ находится, пожалуй, крупнейшая хакерская организация «GForce Pakistan», которая взяла на себя ответственность за взлом сайта «Jerusalembooks.com» в 2006 году.

Наряду с хакерскими организациями против Израиля «сражается» масса талантливых хакеров-одиночек, одним из которых является ранее упомянутый персонаж, известный как Dodi. Именно он 3 ноября 2006 года нарушил работоспособность компании NetVision, которая выступает в качестве основного интернет-провайдера страны; на ее долю приходится 2/3 сетевого трафика Израиля³.

На первый взгляд «оружие нового тысячелетия» имеет огромный потенциал, однако, аналитики полагают, что виртуальному пространству Израиля еще предстоит ощутить всю тяжесть кибер-войны с хакерами арабских государств. Массовые «Ddos-атаки» (выведение из строя сервисов по обслуживанию Интернет-ресурсов), подмена содержимого Web-сайтов (известно как «defacement»), рассылка спама (или «mail bombing») и иные «увлечения»

¹ Позолотин, В.В. Информационно-идеологическое противостояние в зоне палестино-израильского конфликта / В.В. Позолотин. М.: Институт Ближнего Востока, 2000. С. 14.

² В арабо-израильскую войну вступили Интернет-подпольщики [Электронный ресурс] // «Рол-Новости» со ссылкой на Netoscope.ru. URL: http://www.rol.ru/it/news/00/11/16_852.html, Режим доступа: свободный. (Дата обращения: 28.03.2017)

³ Там же.

пропалестинских хакеров за последние годы не нанесли серьезного вреда. Но когда эти атаки приобретают массовый характер, они способны подорвать работоспособность сети-Интернет в глобальном масштабе¹.

Стоит отметить, что на конец первого десятилетия XX века 2/3 информационных атак пришлось на Израиль и его союзников, главным образом – США. Вместе с тем, специалисты по компьютерной безопасности, в частности – Питер Соммер – член Центра исследований по компьютерной безопасности при Лондонской Экономической Школе, полагают, что активность политически настроенных хакеров будет лишь возрастать, а главная цель их атак – создание угрозы государственной инфраструктуре².

Однозначно, говоря о значимости кибервойн, не стоит преувеличивать их опасность, ведь каждый социально-, политически- и экономически важный объект зачастую имеет надежную систему защиты от взлома, имеет дублированные системы передачи данных без прямого Интернет-соединения, а обслуживающий персонал незамедлительно реагирует на поступившие угрозы.

На сегодня наибольшую угрозу представляют не столько новейшие методы кибер-атак, сколько их количество и внезапность. Зачастую цель подобных акций заключается в выведении из строя, путем вирусных атак, сотен, а то и тысяч компьютеров. Результатом подобных атак является как финансовый урон, так и деморализация людей (владельцев пострадавших компьютеров), т.к. они лишаются привычного источника получения информации, общения и развлечения. Таким образом, главная задача кибертеррористов - не материальный вред, а психологическое давление.

СМИ играют немаловажную роль в столь тревожном восприятии кибертеррористов. Нередко бывает так, что кибер-атаки происходят по заказу самих производителей оборудования с целью увеличения рынка сбыта защитного

¹ Когда начнется вторая арабо-израильская «кибер-война? [Электронный ресурс] // Lenta.co.il со ссылкой на Israland Новости. URL: <http://www.lenta.co.il/page/230501hack>, Режим доступа: свободный. (Дата обращения: 28.03.2017)

² Хакеры как оружие информационной войны [Электронный ресурс] // Inforum.biz со ссылкой на story.news.yahoo.com. URL: <http://www.inforum.org/profi/archive.php?cat=2>, Режим доступа: свободный. (Дата обращения: 02.04.2017)

программного обеспечения. Так, в начале 2000-х годов сайт Yahoo сделал заявление, что в связи с атаками хакеров потерял около 10 миллиардов долларов. Эксперты назвали данную сумму попросту нереальной, т.к. согласно расчетам, 12 миллионам пользователей пришлось бы совершить транзакции равные 800 долларам. В связи с чем, данное заявление было воспринято как пиар-акция, нежели реальная хакерская атака¹.

Гарантировать абсолютное отсутствие кибер-атак нереально. Ни стоит забывать о деятельности спецслужб, чья задача заключается в противоборстве кибертеррористам. Стоит подчеркнуть, что борьба с кибертерроризмом – одна из сфер международного сотрудничества. Следовательно, односторонние действия какого-либо государства могут привести лишь к всплеску беззакония в рамках киберпространства.

2.2 Поиски путей противодействия информационным войнам на Ближнем Востоке, и их потенциал

Ближний Восток – это термин, придуманный европейцами для обозначения «восточных» территорий, наиболее близких к Европе².

Говоря обобщенно, можно сказать, что Ближний Восток – это западная часть Азии и северо-восток Африки.

Вообще же общепринятого понимания термина Ближний Восток не существует. В каждой стране данный термин понимают по-своему. Согласно мнению Е. Сатановского каждая имперская столица имела свое видение мира, каждая академия унаследовала это видение от своей империи, а современные постмодернистские научные школы привнесли в это немало путаницы³.

¹ Электронный джихад. Как сражаются палестинские и израильские хакеры [Электронный ресурс] // «Деловая пресса» со ссылкой на «Московские новости». URL: http://www.businesspress.ru/newspaper/article_mId_1081_aId_45149.html, Режим доступа: свободный. (Дата обращения: 02.04.2017)

² Mahan, A.T. The Persian Gulf and International Relations / A.T. Mahan // National review. 1902.

³ Сатановский, Е. Россия и Ближний Восток. Котел с неприятностями / Е. Сатановский. М.: Эксмо, 2012. С. 8.

Ближний Восток издавна отличался наличием множества различных религий и этнических групп. Нередко это приводило к этноконфессиональным конфликтам, хотя, сам по себе факт религиозного и этнического разнообразия не порождает неизбежного противостояния. Нередко за этими конфликтами скрываются политические и экономические причины, которые лишь маскируются религиозными лозунгами.

Иудеи с древних времен проживали на территории Палестины. Особенно после разрушения Второго храма римлянами в Иерусалиме часть иудеев бежала в Палестину и в другие страны Ближнего Востока.

В конце XIX века среди евреев возникло движение за возвращение в Палестину и создание там своего государства. Это стремление претворилось в жизнь сразу после Второй мировой войны, когда образовалось государство Израиль (1948 год). С самого своего возникновения это государство стало причиной неутрачиваемых конфликтов на Ближнем Востоке между мусульманами (всех направлений, одинаково враждебно настроенных по отношению к Израилю) и самим Израилем.

Причиной конфликта стал территориальный спор между евреями и арабами за обладание Эрец-Исраэль (историческая страна еврейского народа). Что, в свою очередь, повлекло череду этнических и религиозных противоречий¹.

Существует также проблема «оккупированных территорий» (имеется в виду оккупированных Израилем), которые арабы и евреи оспаривают друг у друга (Иерусалим, Голанские высоты и т.д.)².

Противодействие информационным войнам имеет такую же древнюю историю, как и сама информационная агрессия. Арабо-израильский конфликт в течение полувека пытались разрешить стандартными средствами войны - самолетами и танками. Однако открылся иной фронт - киберпространство. И если раньше основной акцент в таком противодействии делался на репрессивных

¹ Пырлин, Е.Д. 100 лет противоборства. Генезис, эволюция, современное состояние и перспективы решения палестинской проблемы / Е.Д.Пырлин. М.: РОССПЭН, 2001. С. 48.

² Там же.

механизмах, лишении физических возможностей получения противоположной информации (типа изъятия радиоприемников или глушения радиопередач), то сегодня акцент делается на информационном противодействии. Как говорит Ким Гхаттас из MSNBC: представители Израиля и Палестины ведут ожесточенную виртуальную битву, неустанно обрушивая поток дезинтегрирующей информации друг на друга, путем нажатия на гашетку нового оружия информационной эры - клавишу мыши¹.

Цензура - один из эффективных методов борьбы на информационном фронте. Иногда, однако, слишком явные и грубые методы приводят к «голу в свои ворота».

Кто руководит цензурой в Израиле и Палестине. Цель работы не в этом, но можно с большой долей уверенности предположить, что с обеих сторон требования определяются правительством и спецслужбами. Иногда их директивы «просачиваются», иногда их содержание можно «вычислить» из сообщений журналистов.

Например, когда власти Израиля 31 января 2002 года ввели строгую цензуру на радио в связи с непрекращающейся интифадой, журналистов отдела арабского вещания «Радио Израиля» Reshet Dalet ознакомили с директивой следующего содержания²:

- нельзя использовать слово «жертва», говоря о мирных палестинских гражданах, убитых во время интифады. Вместо слова "жертва" ведущим следует говорить «убитый»;
- при цитировании палестинцев и арабов следует воздерживаться от употребления слов, которые могут быть расценены как свидетельство поддержки радиожурналистом их высказываний;

¹ Дисабатино, Дж. Кибервойна на Ближнем Востоке / Дж. Дисабатино // Computerworld Россия. 2000. №42. С.14.

² Новый способ улучшения имиджа Израиля: попытки цензуры СМИ [Электронный ресурс] // Новости Израиля. URL: <http://news.israelinfo.co.il/kaleidoscope/66661>, Режим доступа: свободный. (Дата обращения: 25.05.2017)

- не следует употреблять выражение «по словам», комментируя заявления израильских официальных лиц, в том числе военного руководства, поскольку в результате может сложиться впечатление, что вы подвергаете их сомнению. В то же время нет никаких ограничений на использование этого выражения, если речь идет о высказываниях палестинцев;

- когда официальный представитель какой-либо израильской структуры, в том числе вооруженных сил, опровергает «ложь и клевету, например, в отношении событий в Дженине, недостаточно употребить слово «опроверг», как это было сделано в некоторых репортажах радиостанции». Вместо этого журналисты должны использовать слова, наглядно демонстрирующие лживость подобного освещения событий, повторив в конце репортажа следующую фразу: «Официальный представитель подчеркнул, что эти клеветнические заявления полностью лживы и необоснованны»;

- когда какой-либо депутат Кнессета опровергает или выражает свое несогласие с заявлениями премьер-министра, «никогда не следует употреблять слова «опроверг» или «не согласился». Вместо этого нужно говорить «возразил» или «высказал свои возражения»;

- не следует употреблять слово «убийство» по отношению к палестинским активистам. Вместо этого нужно использовать слово «уничтожение», когда речь идет о действиях израильской армии, которые сама она называет «точечной ликвидацией».

Директивы напоминают нам о пропагандистской кампании в Чечне, когда речь комментаторов стала в одночасье меняться.

Формально, как и в Израиле, в Палестине соблюдается свобода слова. Тем не менее, западные источники отмечают случаи силового давления на журналистов. Можно даже сказать, что палестинские методы несколько грубее.

Несмотря на заявленную терпимость к различным политическим взглядам и критике, в Палестинской автономии ограничивают свободу слова и прессы. В ряде случаев Автономия приняла меры по ограничению свободы мнений, в

особенности в том, что касалось прав человека и обвинений в коррупции. На территории Палестинской автономии, свобода прессы определяется законом от 1995 года, который не в состоянии достаточно защитить ее¹. Службы безопасности Палестинской автономии ущемляют свободу прессы еще и тем, что закрывают издания, запрещают публикацию материалов, а также периодически оказывают давление и задерживают представителей СМИ. Палестинские комментаторы и группы по правам человека говорят, что, как следствие этой практики, явление самоцензуры среди журналистов очень распространено².

С самого создания в 1994 году Палестинская автономия усиливала нажим на свободу прессы путем применения таких методов, как арест и задержание журналистов различными службами безопасности. Многие арестанты были лишены права контакта с кем-либо, а некоторые оказались жертвами пыток и плохого обращения. Арестованным редко предъявляют ордер или сообщают причину ареста. Однако, сам факт того, что арест производится спустя часы или дни после опубликования ими «спорного» материала или написания критической статьи, оставляет мало места для сомнений в истинной причине их ареста. Часто арестантам не было понятно, кто именно распорядился об их аресте, исходила ли инициатива от служб безопасности или от самого президента (Ясира Арафата). Во многих случаях задержанным устно объявляли, что их не отпускают «по высшему указу». Среди арестованных были журналисты и академики, политические активисты и юристы, представители правительств и профсоюзные работники, а так же религиозные деятели³.

¹ Будущее Палестинской автономии: власти и "Хамас"; обзор палестинской прессы [Электронный ресурс] // Радио Свобода. URL: <https://www.svoboda.org/a/24199356.html>, Режим доступа: свободный. (Дата обращения: 26.05.2017)

² Госдепартамент представил ежегодный доклад о правах человека в мире [Электронный ресурс] // Русская служба «Голоса Америки». URL: <https://www.golos-ameriki.ru/a/state-department-human-rights/3284365.html>, Режим доступа: свободный. (Дата обращения: 28.05.2017)

³ Будущее Палестинской автономии: власти и "Хамас"; обзор палестинской прессы [Электронный ресурс] // Радио Свобода. URL: <https://www.svoboda.org/a/24199356.html>, Режим доступа: свободный. (Дата обращения: 26.05.2017)

ПНА нарушала право на свободное выражение мнений и другими способами. Со многими журналистами службы безопасности грубо обращались при выполнении их служебных обязанностей. Газеты, исследовательские центры, агентства новостей, телевизионные и радиостанции - неоднократно закрывались на несколько дней и даже недель. Так, в мае 2008 года 2 частных радиостанции на Западном берегу и 3 частных телевизионных станции были закрыты палестинской полицией на несколько дней¹.

Чтобы избежать всех проблем, описанных выше, некоторые палестинские журналисты признают, что практикуют самоцензуру, выражающуюся либо в преподнесении истории в определенной манере, либо в игнорировании определенных событий. Даже в случаях, когда журналист готов рискнуть, его редактор может не захотеть брать на себя ответственность за публикацию критической статьи².

Наиболее жесткие замечания звучат со стороны израильской «Палестинской группы наблюдения за правами человека»³. ПГНПЧ осознает серьезность распространившегося явления самоцензуры среди палестинских журналистов, что не только не позволяет обнародовать правду, но также и ограничивает свободу мышления. Журналисты на территории Палестинской автономии сталкиваются с внешней цензурой, ограничивающей свободу мнения и выражения. Они начинают практиковать самоцензуру, что лимитирует инициативу и осмысление тех материалов, которые могут попасть за очерченные границы.

Все это сделало местную прессу похожей на попугаев, повторяющих то, что от них ожидают услышать, не задавая никаких вопросов и не критикуя. «Самоцензура» является явлением более серьезным, чем цензура внешняя, т.к.

¹ Имеются доказательства того, что палестинские силовые структуры превышают полномочия [Электронный ресурс] // Amnesty International. URL: <https://amnesty.org.ru/ru/2008-03-14-palestina/>, Режим доступа: свободный. (Дата обращения: 27.05.2017)

² Там же.

³ Самоцензура распространена среди палестинских работников средств массовой информации [Электронный ресурс] // Ассоциация русскоязычных журналистов Израиля. URL: <http://iarj.org.il/branja/samotsenzura-rasprostranena-sredi-palestinskih-rabotnikov-sredstv-massovoj-informatsii/>, Режим доступа: свободный. (Дата обращения: 01.06.2017)

она не только ограничивает публикацию материалов, но также изрядно подавляет саму способность думать, анализировать и писать. Никто не станет тратить время на материал, о котором заранее известно, что его не опубликуют.

Самоцензура усиливается, когда журналист слышит о коллеге, пострадавшем от служб безопасности за переступание красной черты.

Нарушения прав палестинских журналистов (допущенные полицией, разведкой, службой национальной безопасности, и различными агентствами) за переступание красной черты бывают разными. Из 50 различных нарушений, задокументированных ПГНПЧ наблюдалось следующее процентное распределение¹:

- Огнестрельное ранение: 2%;
- Избиение: 12%;
- Конфискация или уничтожение камеры: 6%;
- Конфискация пленок: 8%;
- Вызовы, арест или содержание под стражей: 68%.

Однако не только внутренние причины влияют на возникновение и развитие этнорелигиозных конфликтов на Ближнем Востоке. Не последнее место в этом (а, по мнению некоторых экспертов, – даже первое) занимают внешние влияния, прежде всего влияние США.

Политика США в данном регионе самым тесным образом связана с нефтяным фактором, ведь Ближний Восток – это один из главных нефтедобывающих регионов мира.

Постоянное активное вмешательство США в дела на Ближнем Востоке связано с тем, что Соединенные Штаты жизненно заинтересованы в том, чтобы ближневосточная нефть продолжала беспрепятственно и относительно дешево поступать на Запад. Современная глобальная экономика, созданная после Второй мировой войны, базируется на фундаменте сравнительно недорогой нефти, и если

¹ Свобода слова на Ближнем Востоке [Электронный ресурс] // Форум ТВС. URL: <http://www.forum-tvs.ru/index.php?showtopic=2996>, Режим доступа: свободный. (Дата обращения: 01.06.2017)

этот фундамент исчезнет, то глобальная, а следовательно и американская экономика, которая является ее лидером, попадут в полосу жестокого кризиса¹.

По этой причине США и другие западные страны в значительной степени зависят от энергетических ресурсов Ближнего Востока, по причине чего постоянно вмешиваются в дела этого региона, нередко становясь (как в случае с Ираком и Сирией) главными причинами возникновения конфликтов.

Такое вмешательство извне с явно корыстными целями не может не вызывать противодействия со стороны населения и властей ближневосточных государств. Политика Запада приводит к радикализации ислама, появлению различных экстремистских группировок. Иногда такие группировки с различными целями непосредственно создаются западными спецслужбами, либо поддерживаются ими.

Не обладая военной мощью и технологиями, относительно западных стран, ближневосточные акторы идут по пути асимметричного ответа, используя терроризм и тактику партизанской войны в случае прямого военного столкновения, как это и произошло в Ираке.

В итоге, по причине активного и постоянно усиливавшегося вмешательства извне Ближний Восток стал восприниматься как конфликтный регион планеты.

Исходя из всего вышесказанного, конфликт между Израилем и Палестиной представляется ярким примером информационной войны. Он является и глобальным, т.к. затрагивает интересы десятка государств².

Арабо-израильское противостояние приобрело новое дыхание во время изменения статуса Палестины при Организации Объединенных Наций. Статус Палестины был изменен с организации - наблюдателя на полноправное государство – наблюдатель. На этом этапе информационной войны действия Израиля, вместе с его американскими коллегами, не увенчались успехом. Показателем провала стала поддержка лишь 9 государств – членов Генеральной

¹ Примаков, Е.М. Конфиденциально: Ближний Восток на сцене и за кулисами (вторая половина XX и начало XXI века) / Е.М. Примаков. М.: Российская газета, 2006. С. 67.

² Там же. С. 69.

ассамблеи ООН. Причем 4 из них являлись государствами Карибского бассейна с режимом правления, подвластным США.

На протяжении последнего столетия Соединенные Штаты активно способствуют нормализации отношений Израиля с его арабскими соседями и мусульманским миром в целом. Действительно, после войны в Персидском заливе (1991 г.) возникла совершенно новая структура взаимоотношений между Израилем и арабскими государствами. Активно развивались дипломатические и экономические контакты Израиля с Тунисом, Оманом, Марокко и Катаром. Однако это сотрудничество в 2000 г. было приостановлено в связи с началом первой Интифады арабо-израильского противостояния. Более того, значительно ухудшились отношения Израиля с его главными арабскими партнерами в регионе – Египтом и Иорданией.

Следует также отметить, сегодня дипломатические отношения Израиль поддерживает с 156 странами мира, 36 государств не имеют дипломатических отношений с государством Израиль, из них 20 государств, являются членами Арабской Лиги, а не признает факта существования государства Израиль 21 страна¹.

Политика Израиля в отношении арабских государств остается жесткой. В частности арабскими странами перед Организацией Объединенных Наций был поставлен вопрос о судьбе беженцев. Израиль прокомментировал ситуацию следующими словами: беженцы должны укореняться в странах пребывания; о возвращении арабских беженцев на территории Израиля не может быть речи².

Сегодня Соединенные Штаты являются основным внешним фактором в ближневосточном регионе, который признают как Израиль, так и Палестинская администрация. Именно американское посредничество в ближайшем будущем будет предопределять динамику арабо-израильских переговоров.

¹ Внешняя политика Израиля [Электронный ресурс] // PRO-SRAEL. URL: <http://www.pro-israel.ru/politika-israelya.html>, Режим доступа: свободный. (Дата обращения: 23.05.2017)

² План «Дорожная карта» [Электронный ресурс] // Сайт ООН. URL: <http://www.un.org/ru/peace/palestine/part6.pdf>, Режим доступа: свободный. (Дата обращения: 26.05.2017)

Но успех, который был достигнут Вашингтоном в урегулировании арабо-израильского конфликта в прошлом, был основан на американской роли честного брокера. И только восстановление этого имиджа позволит Соединенным Штатам вернуть себе доверие и играть в мирном процессе действительно эффективную роль.

Прежде всего, Соединенные Штаты не должны отходить от своего исторического обязательства по лозунгу «территория в обмен на мир». Ведь только Вашингтон способен убедить Израиль в необходимости освобождения территорий на Западном берегу и в секторе Газа в обмен на гарантии безопасности. Такая политика будет полностью соответствовать моральным и стратегическим обязательствам США перед Израилем, т.к. возврат израильтян в четко определенные и международно-признанные границы сделает их гораздо более защищенными¹.

Вашингтон должен противостоять насилию и актам террора со стороны палестинцев. Для этого Соединенным Штатам следует признать необходимость размещения миротворческих сил ООН в регионе для разделения противоборствующих сторон и прекращения насилия. США следует способствовать демократизации палестинского общества и делать все возможное для повышения жизнеспособности Палестинской автономии, поощряя развитие палестинской экономики и преодоления ее зависимости от израильской².

Как мы уже выяснили, основой обеспечения эффективной борьбы с кибертерроризмом/информационно-психологическим воздействием является создание эффективной системы взаимосвязанных мер по выявлению, предупреждению и пресечению такого рода деятельности. Для борьбы с терроризмом во всех его проявлениях работают различные антитеррористические органы. Особое внимание борьбе с терроризмом уделяют развитые страны мира, считая его едва ли не главной опасностью для общества. Но полностью

¹ Довгялло, М.А. Роль США в урегулировании Ближневосточной проблемы / М.А. Довгялло. М.: Наука, 2009. С. 73.

² Там же. С. 80.

обезопасить общество от террористов невозможно, можно лишь снизить угрозу превентивным контролем за «интересными» для террористов местами и борьбой с непосредственными исполнителями террористических актов. Задача состоит в том, чтобы сузить варианты действий террористов и контролировать те, что останутся. Но тотальная слежка за всеми, как, например, происходит в рамках палестинской проблемы - это нарушение прав человека.

Но существует и обратная сторона данного вопроса: если же не устанавливать тотальный контроль, то предпосылки, существующие сегодня гласят о том, что преступления в сфере высоких технологий могут выйти на качественно новый уровень. Так нет необходимости захватывать самолет с заложниками. Проще угрожать жизни всех, кто находится в небе, через компьютер, управляющий полетами. Если политический деятель заболел и попал в больницу, вместо покушения на него с помощью винтовки или взрывчатки, проще через Интернет взломать защиту локальной сети госпиталя и добраться до системы жизнеобеспечения больного. Небольшое изменение в программе - и результат достигнут. Десятки тысяч людей могут оказаться заложниками, если террорист через сеть вмешается в работу промышленного производства.

В качестве примера можно привести 16 медицинских учреждений, которые подверглись хакерским атакам 12 мая 2017 года. В частности, на взломанных компьютерах появлялось сообщение с требованием заплатить выкуп в размере 300 долларов, иначе, все информация будет потеряна. По данным NHS (Национальная служба здравоохранения Великобритании), во взломанных учреждениях были недоступны данные о пациентах, рецептах и записях на прием, а также заблокированы телефонные линии и почтовые сервисы. Отменены сотни запланированных хирургических операций¹. Все ведущие государства мира серьезно обеспокоены рассматриваемыми проблемами.

¹ Хакеры взломали британские медучреждения с помощью измененных программ АНБ [Электронный ресурс] // РИА Новости. URL: <https://ria.ru/world/20170512/1494221941.html>, Режим доступа: свободный. (Дата обращения: 23.05.2017)

Что касается арабо-израильского конфликта, особенно в сегодняшней ситуации, можно с высокой долей вероятности сказать, что стороны вряд ли сами сядут за стол переговоров. И на современном этапе был бы целесообразен не односторонний нажим на противоборствующие стороны со стороны США, являющихся стратегическим партнером Израиля и страной, обладающей мощью в политической, экономической и сфере высоких технологий, а стимулирование мирного процесса силами всего мирового сообщества. Для этого в ближневосточный мирный процесс наряду с США должны быть привлечены, прежде всего, Россия и Европейский союз, а также другие акторы международных отношений, обладающие определенным влиянием. Необходимо также повысить активность в обсуждении ближневосточных проблем на трибунах различных международных организаций (как региональных, так и глобальных) и, прежде всего, ООН.

ЗАКЛЮЧЕНИЕ

Таким образом, внедрение информационных технологий во все сферы жизни общества привело мир в конце XX столетия в информационное общество, для которого характерен переизбыток информации. Однако выбрать наиболее существенную для принятия решений в этом потоке информации становится довольно трудно, поскольку, во-первых, информация постоянно обновляется и подвергается интерпретациям и переинтерпретациям, во-вторых, информационно-коммуникационные технологии ставят под вопрос достоверность источника в силу своей природы, и в-третьих, в основе производства информации высокими технологиями лежит медиа образ. Все это ведет к тому, что человек лишается самостоятельного мышления, превращая его в послушного ученика экспертов, которые наиболее часто оказываются агентами влияния тех или иных заинтересованных лиц. Возникают невиданные ранее возможности овладения капиталом и властью путем информационных операций, которые приобретают характер войн. Традиционное обществознание оказалось отчасти не готово к этому и не смогло снабдить членов общества знаниями об управлении информационной борьбой. Те же, кто овладел этими знаниями, приобретают кажущуюся извне магической способность использовать любые изменения в свою пользу, иными словами – реализовывают стратегию «мягкой власти».

Стоит отметить, что информационно-психологическая составляющая компонента имела во всех войнах и противостояниях человечества. Ее содержание было заключено в основном в действиях противостоящих сторон по распространению дезинформации или информации для воздействия на намерения и ориентацию населения, личного состава вооруженных сил и лиц принимающих решения, с целью формирования общественного мнения, выгодного для воздействующей стороны.

Арабо-израильский конфликт наглядно показал столкновение интересов не только Израиля и Палестины. Очевидное противостояние происходит между Российской Федерацией, с одной стороны, и США и Евросоюзом с другой. И,

если военные действия ведутся непосредственно между палестинцами и израильтянами, то информационное противостояние наблюдается в глобальном масштабе.

На сегодняшний день, главный результат информационной войны между Палестиной и Израилем заключается в создании стойкой ненависти между рядовыми гражданами этих государств, дезинтеграции арабо-израильского общества, а также формирование устойчивого образа врага всевозможными способами пропаганды «нужных» воззрений. Причем сила последних такова, что даже если конфликт будет урегулирован в ближайшее время, на избавление от этих стереотипов потребуются долгие годы напряженной работы.

Огромную роль здесь, конечно, сыграло развитие СМИ, и в особенности, сети Интернет и телевидения. Интернет стал оружием ужасной силы в руках тех, кто имеет к нему доступ, поскольку вобрал в себя такие важные факторы «всемогущего» коммуникационного канала как моментальность, оперативность информации и визуальную стимуляцию. С его помощью можно наиболее эффективно вершить судьбы людей, поскольку мало кто не поверит глазам своим. Однако не стоит упускать из вида и программно-технические средства ведения «кибервойны», а именно: компьютерные вирусы, логические бомбы, взломы персональных сайтов и т.д.

Гарантировать абсолютное отсутствие кибератак нереально. Ни стоит забывать о деятельности спецслужб, чья задача заключается в противоборстве кибертеррористам. Стоит подчеркнуть, что борьба с кибертерроризмом – одна из сфер международного сотрудничества. Следовательно, односторонние действия какого-либо государства могут привести лишь к всплеску беззакония в рамках киберпространства.

Однозначно можно сказать, Интернет-порталы с обеих сторон не предоставляют аудитории всесторонний информационный продукт, но зачастую такие порталы, как Isralife.com или Palinfo.com - единственный источник информации с оккупированной территории. Кроме того, опыт освещения арабо-

израильского конфликта является наглядной картинкой и для российских СМИ, журналисты которых тоже зачастую политически ангажированы.

Информационные войны становятся реальностью современности. В сегодняшней ситуации, можно с высокой долей вероятности сказать, что стороны вряд ли сами сядут за стол переговоров. На современном этапе был бы целесообразен не односторонний нажим на противоборствующие стороны со стороны США, а стимулирование мирного процесса силами всего мирового сообщества. Для этого в ближневосточный мирный процесс наряду с США должны быть привлечены, прежде всего, Россия и Европейский союз, а также другие акторы международных отношений, обладающие определенным влиянием. Необходимо также повысить активность в обсуждении ближневосточных проблем на трибунах различных международных организаций (как региональных, так и глобальных) и, прежде всего, ООН.

Итак, в данной выпускной квалификационной работе был рассмотрен феномен информационных войн. Мы изучили историю возникновения понятия «информационная война», а также проследили его взаимосвязь со стратегией «мягкой власти». Помимо этого рассмотрели механизмы воздействия «информационных атак», привели современные примеры техник ведения информационных войн.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Источники:

1. Арабские СМИ ведут джихад против Израиля [Электронный ресурс] // Центральный Еврейский Ресурс. URL: <http://forum.sem40.ru/>, Режим доступа: свободный. (Дата обращения: 07.04.2017)
2. Более 1,3 млн. подключенных к интернету компьютеров в Израиле, т.е. больше чем во всех арабских странах вместе взятых [Электронный ресурс] // Компьюлента. Режим доступа: свободный. (Дата обращения: 23.03.2017)
3. Будущее Палестинской автономии: власти и "Хамас"; обзор палестинской прессы [Электронный ресурс] // Радио Свобода. URL: <https://www.svoboda.org/a/24199356.html>, Режим доступа: свободный. (Дата обращения: 26.05.2017)
4. В арабо-израильскую войну вступили Интернет-подпольщики [Электронный ресурс] // «Рол-Новости» со ссылкой на Netoscope.ru. URL: http://www.rol.ru/it/news/00/11/16_852.html, Режим доступа: свободный. (Дата обращения: 28.03.2017)
5. Внешняя политика Израиля [Электронный ресурс] // PRO-SRAEL. URL: <http://www.pro-israel.ru/politika-israelya.html>, Режим доступа: свободный. (Дата обращения: 23.05.2017)
6. Госдепартамент представил ежегодный доклад о правах человека в мире [Электронный ресурс] // Русская служба «Голоса Америки». URL: <https://www.golos-ameriki.ru/a/state-department-human-rights/3284365.html>, Режим доступа: свободный. (Дата обращения: 28.05.2017)
7. Зачем Усаме порносайт? [Электронный ресурс] // Центриальный Еврейский Ресурс. URL: www.sem40.ru, Режим доступа: свободный. (Дата обращения: 24.03.2017)

8. Израиль и электронный джихад [Электронный ресурс] // Правда.Ru. URL: <http://www.pravda.ru/article/803616.html>, Режим доступа: свободный. (Дата обращения: 24.03.2017)
9. Имеются доказательства того, что палестинские силовые структуры превышают полномочия [Электронный ресурс] // Amnesty International. URL: <https://amnesty.org.ru/ru/2008-03-14-palestina/>, Режим доступа: свободный. (Дата обращения: 27.05.2017)
10. Информационная война и цифровой мир [Электронный ресурс] // Сайт Независимой газеты. URL: https://www.ng.ru/stsenarii/2016-04-26/12_infowar.html, Режим доступа: свободный. (Дата обращения: 23.03.2017)
11. Кибервойна на Ближнем Востоке. Противостояние между израильтянами и палестинцами переместилось в Сеть [Электронный ресурс] // ComputerWorld. URL: <http://www.osp.ru/cw/2000/42/7800/>, Режим доступа: свободный. (Дата обращения: 28.03.2017)
12. Когда начнется вторая арабо-израильская «кибер-война?» [Электронный ресурс] // Lenta.co.il со ссылкой на Israland Новости. URL: <http://www.lenta.co.il/page/230501hack>, Режим доступа: свободный. (Дата обращения: 28.03.2017)
13. Новый способ улучшения имиджа Израиля: попытки цензуры СМИ [Электронный ресурс] // Новости Израиля. URL: <http://news.israelinfo.co.il/kaleidoscope/66661>, Режим доступа: свободный. (Дата обращения: 25.05.2017)
14. План «Дорожная карта» [Электронный ресурс] // Сайт ООН. URL: <http://www.un.org/ru/peace/palestine/part6.pdf>, Режим доступа: свободный. (Дата обращения: 26.05.2017)
15. Портрет настоящей кибервойны [Электронный ресурс] // Information Security со ссылкой на inosmi.ru. URL: http://www.itsec.ru/newstext.php?news_id=60110, Режим доступа: свободный. (Дата обращения: 19.03.2017)

16. Рейтинг «мягкой силы». The Soft Power 30 [Электронный ресурс] // Официальный сайт ИМЭМО. URL: http://www.imemo.ru/index.php?page_id=502&id=1773, Режим доступа: свободный. (Дата обращения: 07.03.2017)
17. Самоцензура распространена среди палестинских работников средств массовой информации [Электронный ресурс] // Ассоциация русскоязычных журналистов Израиля. URL: <http://iarj.org.il/branja/samotsenzura-rasprostranena-sredi-palestinskih-rabotnikov-sredstv-massovoj-informatsii/>, Режим доступа: свободный. (Дата обращения: 01.06.2017)
18. Свобода слова на Ближнем Востоке [Электронный ресурс] // Форум ТВС. URL: <http://www.forum-tvs.ru/index.php?showtopic=2996>, Режим доступа: свободный. (Дата обращения: 01.06.2017)
19. Хакеры взломали британские медучреждения с помощью измененных программ АНБ [Электронный ресурс] // РИА Новости. URL: <https://ria.ru/world/20170512/1494221941.html>, Режим доступа: свободный. (Дата обращения: 23.05.2017)
20. Хакеры взломали сайт Шарона и украли базу данных [Электронный ресурс] // Lenta.ru. URL: <http://lenta.ru/internet/2001/01/31/sharon/>, Режим доступа: свободный. (Дата обращения: 27.03.2017)
21. Хакеры как оружие информационной войны [Электронный ресурс] // Inforus.biz со ссылкой на story.news.yahoo.com. URL: <http://www.inforus.org/profi/archive.php?cat=2>, Режим доступа: свободный. (Дата обращения: 02.04.2017)
22. Электронный джихад [Электронный ресурс] // Новости от Новикова со ссылкой на nationalreview.com. URL: <http://content.mail.ru/arch/8016/156566.html>, Режим доступа: свободный. (Дата обращения: 24.03.2017)
23. Электронный джихад. Как сражаются палестинские и израильские хакеры [Электронный ресурс] // «Деловая пресса» со ссылкой на «Московские новости». URL:

http://www.businesspress.ru/newspaper/article_mId_1081_aId_45149.html, Режим доступа: свободный. (Дата обращения: 24.03.2017)

24. Soft Power - мягкая сила «made in USA» [Электронный ресурс] // Персональный сайт Сергея Халеменика. URL: <http://www.chelemendik.ru/ShowDoc.php%3Fd%3D620>, Режим доступа: свободный. (Дата обращения: 18.03.2017)

Литература:

25. Абдеев, Р. Ф. Философия информационной цивилизации / Р. Ф. Абдеев. М.: ВЛАДОС, 1994. 336 с.

26. Бабаева, Ю.Д. Интернет: воздействие на личность / Ю.Д. Бабаева, А.Е. Войскунский, О.В. Смылова. М.: Можайск-Терра, 2000. 54 с.

27. Балугев, Д.Г. Роль «новых СМИ» в современных политических процессах / Д.Г. Балугев, А.А. Новоселов. Нижний Новгород, 2012. 196 с.

28. Бернейс, Э. Манипуляция общественным мнением: как и почему / Э. Бернейс // Полис: политические исследования. 2012. №4. С. 149-154.

29. Бовин, А. 5 лет среди евреев и мидовцев. // А. Бовин М.: Захаров, 2002. 207 с.

30. Брусницын, Н.А. Информационная война и безопасность / Н.А. Брусницын. М.: Вита-Пресс, 2001. 280 с.

31. Вартанова, Е.Л. Медиа-экономика в информационном обществе / Е.Л. Вартанова. М.: Информационное общество, 2011. 390 с.

32. Винер, Н. Кибернетика / Н. Винер. М.: Наука, 1968. 124 с.

33. Гриняев, С. Концепция ведения информационной войны в некоторых странах мира / С. Гриняев // Зарубежное военное обозрение. 2002. №2. С. 11-15.

34. Девяткина, А.Г. Информационные войны в современных международных отношениях / А.Г. Девяткина // Актуальные проблемы современных международных отношений. 2014. №3. С. 54-59.

35. Дисабатино, Дж. Кибервойна на Ближнем Востоке / Дж. Дисабатино // Computerworld Россия. 2000. №42. С. 5-18.
36. Довгялло, М.А. Роль США в урегулировании Ближневосточной проблемы / М.А. Довгялло. М.: Наука, 2009. 269 с.
37. Жуков, В. Взгляды США на ведение информационной войны / В. Жуков // Зарубежное военное обозрение. 2001. №1. 124 с.
38. Кастельс, М. Информационная эпоха: экономика, общество и культура / М. Кастельс. Пер. с англ. под науч. ред. О. И. Шкаратана. М.: ГУ ВШЭ, 2000. 607 с.
39. Кравченко, С.А. Социология: парадигмы через призму социологического воображения / С.А. Кравченко. Учеб.пособие. М.: Экзамен, 2007. 560 с.
40. Маничев, С.А. Мифология в политических технологиях / С.А. Маничев // Общество и политика: Современные исследования, поиск концепций. Под ред. В. Ю. Большакова. СПб.: СПбГУ, 2004. 246 с.
41. Манойло, А.В. Государственная информационная политика в особых условиях / А.В. Манойло. Монография М.: МИФИ, 2003. 203 с.
42. Маринко, Г.И. Управленческий консалтинг / Г.И. маринко. Учеб.пособие. М.: Инфра-М, 2005. 247 с.
43. Най, Дж.С. Кибер-война и мир. [Электронный ресурс] // ИноСМИ. URL: <http://www.inosmi.ru/usa/20120417/190643982.html>, Режим доступа: свободный. (Дата обращения: 11.03.2017)
44. Най, Дж.С. Гибкая власть. Как добиться успеха в мировой политике / Дж.С. Най. Новосибирск-М.: Фонд социопрогностических исследований «Тренды», 2006. 243 с.
45. Панарин, И.Н. Первая мировая информационная война. Развал СССР / И.Н. Панарин. СПб.: Питер, 2010. 390 с.
46. Панарин, Н.И. Информационная война и власть / Н.И. Панарин. М.: Мир безопасности, 2016. 437 с.

47. Погорельский, М. Современная военная журналистика: опыт, проблемы, перспективы / М. Погорельский, И. Сафранчук. М.: Гендальф, 2002. 218 с.
48. Позолотин, В.В. Информационно-идеологическое противостояние в зоне палестино-израильского конфликта / В.В. Позолотин. М.: Институт Ближнего Востока, 2000. 64 с.
49. Почепцов, Г.Г. Информационные войны / Г.Г. Почепцов. М.: Рефл-бук, 2001. 567 с.
50. Прилукова, Е.Г. Власть образов: знаково-символическое бытие власти / Е. Г. Прилукова. Челябинск: Изд. центр ЮУрГУ, 2011. 204 с.
51. Примаков, Е.М. Конфиденциально: Ближний Восток на сцене и за кулисами (вторая половина XX и начало XXI века) / Е.М. Примаков. М.: Российская газета, 2006. 412 с.
52. Пырлин, Е.Д. 100 лет противоборства. Генезис, эволюция, современное состояние и перспективы решения палестинской проблемы / Е.Д.Пырлин. М.: РОССПЭН, 2001. 367 с.
53. Радышевский, Д. Электронный джихад / Д. Радышевский // Московские новости. 2002. №4. С. 22-28.
54. Расторгуев, С.П. Философия информационной войны / С.П. Расторгуев. М.: Autoran, 2000. 187 с.
55. Сатановский, Е. Россия и Ближний Восток. Котел с неприятностями / Е. Сатановский. М.: Эксмо, 2012. 340 с.
56. Скуленко, М.И. Журналистика и пропаганда // М.И. Скуленко. Киев, 1987. 96 с.
57. Швец, Д.А. Информационное управление как технология обеспечения информационной безопасности / Д.А. Швец. М.: МГИМО, 2003. 311 с.
58. Шкрабков, В.Н. Информационное оружие и информационные войны / В.Н. Шкрабков. М.: Сориум, 2001. 227 с.
59. Arquilla, J. Looking ahead: preparing for information-age conflict / J.Arquilla, D. Ronfeldt. Athena's camp. Santa Monica, 1997. 214 p.

60. Jefkins, F. Public relations / F.Jefkins, D.Jadin. New York, 2009. 408 p.
61. Mahan, A.T. The Persian Gulf and International Relations / A.T. Mahan // National review. 1902.
62. Nye, Joseph S. Soft Power. The Means to Success in World Politics / Joseph S. Nye. New York: Public Affairs, 2004. 173 p.
63. Rona, T. P. Weapon Systems and Information War / T. P. Rona. Boeing Aerospace Co., Seattle, WA, 1976. 96 p.
64. Shannon, C. A Mathematical Theory of Communication / C. Shannon // Bell System Technical Journal. 1948. 489 p.