Информационная война как угроза национальной безопасности Российской Федерации

Гараева Алина Николаевна
аспирант кафедры международных отношений и зарубежного регионоведения, Нижегородский государственный лингвистический университет имени Н.А. Добролюбова,
alina.garaeva99@yandex.ru

Колобова Светлана Анатольевна
доктор политических наук, доцент, профессор, декан Высшей школы международных отношений и мировой политики, Нижегородский государственный лингвистический университет имени Н.А. Добролюбова

Предпринимается попытка осмысления понятия информационной войны как угрозы национальной безопасности в российском контексте. На примере актуальных международных событий рассматривается вопрос о принципах и методах ведения информационных войн: пропаганда, психологическое воздействие, дезинформация, информационно-идеологическая экспансия, информационно-культурная и экономическая блокада, кибератаки. Автором делается вывод о возрастающей важности данной сферы безопасности Российской Федерации и приводятся примеры мероприятий, проводимых с целью противодействия информационным войнам и укреплению информационной безопасности.
Ключевые слова: информационная война, Российская Федерация, США, международная информационная безопасность, психологическое воздействие, фейковые новости, дезинформация, пропаганда.

Введение

Прежде, чем начать разговор об информационном противоборстве и проблеме международной информационной безопасности, важно отметить, что на современном этапе развития международных отношений под влиянием такого процесса как глобализация, информатизация нашего общества привела к созданию единого глобального информационного пространства, где главным стратегическим национальным ресурсом становится информация и информационные технологии.

На сегодняшний день государствам необязательно обладать военной и экономической мощью, которая являлась приоритетом несколько лет назад. Теперь уровень развития информационного потенциала государства определяет его место в сложившейся системе международных отношений. Борьба за обладание и удержание информационного превосходства занимает одно из важнейших мест в геополитическом противостоянии стран.

Наиболее опасным явлением в информационной сфере является информационная война. Принято считать, что информационная война представляет собой обыкновенное нанесение ущерба информационно-телекоммуникационным системам, хакерские или кибератаки. На самом деле, данное понятие охватывает широкий комплекс мер и способов воздействия, которые оказывают прямое влияние на национальную безопасность государств и ведут подрывную деятельность посредством пропаганды, дипломатии, психологических кампаний, культурной и экономической экспансии, кибератак, и направлены на массированную психологическую обработку населения с целью вывода из строя работы государственных структур.

Методы ведения информационной войны

Наиболее распространенным и эффективным методом информационной войны считается **пропаганда и психологическая война.** В широком смысле это целенаправленное использование пропаганды, а также психологических, дипломатических, военных, экономических и иных средств для воздействия на мнение и поведение противника. Главной целью психологического воздействия является изменение модели мышления и поведения людей, а также групповых норм и общественного сознания в выгодном для противника направлении. Подобные мероприятия сказываются на возможности адекватно воспринимать происходящие события и принимать внутри- и внешнеполитические решения

Примером первой в мире информационно-психологической войны могут служить военные действия США против Ирака в 1991 году, где одним из наиболее эффективных средств воздействия на психологию населения была радиопропаганда, для осуществления которой американцами была разработана доктрина, получившая название Shock and awe («Шок и трепет») [1, С. 3]. Основными целями американцев на Ближнем Востоке, исходя из положений данного документа, выступали: защита Саудовской Аравии, ОАЭ, Катара и Омана от режима Саддама Хусейна; возврат независимости Кувейту; свобода западным судам в районе Персидского залива; демократизация Ирака. Для достижения поставленных целей США осуществили «мощную» психологическую кампанию.

Для эффективности ее проведения был задействован 8-ой батальон из состава 4-ой группы американских офицеров психологических операций, а также специально подготовленная рабочая группа, сформированная в

штабе командования многонациональных сил в Эр-Рияде (Саудовская Аравия) и состоящая из офицеров, отвечающих за психологические операции. В их расположении находились типографии, радиостанции и звуковещательные системы, которые принимали сигналы и радиопередачи, транслируемые коалицией. С 1 января 1991 года радиостанция ВВС увеличила время вещания на арабском языке с 3 до 10 часов в день, а на территории стран, граничащих с Ираком, транслировались передачи радиостанции «Голос свободного Ирака», которые пропагандировали мощь армии США, ее вооружение и военную технику, демонстрировали высокий уровень образования американских военнослужащих, а также критиковали режим Саддама Хусейна.

Во время операции «Буря в пустыне» (Ирак, 1991 год) была распространена не только радиопропаганда, но и печатная и устная пропаганда, эффективность которой сложно недооценить. С помощью Военных Воздушных Сил коалиционной группировки на Ирак и Кувейт было сброшено более 30 миллионов листовок, содержание которых звучало следующим образом: «Сопротивление бесполезно!», «Разгром неизбежен!», «Лучше сдаться в плен» [4, С. 6]. Более 90% опрошенных иракских военнопленных верили в достоверность данной информации, что и побудило их дезертировать. С помощью звуковещательной системы, установленной на вертолете, после проведения передачи «Неизбежность прихода смерти с небес» батальон иракской армии был убежден сдаться. «Эффективное» сочетание радиопропаганды, печатных материалов и психологического воздействия, подкрепленного постоянными бомбардировками и обстрелами, побудило иракские ВС сдаться в плен, а американцам использовать совершенно новые методы ведения информационной войны [13, С. 444].

Следующим методом выступает **дезинформация и распространение фейковых новостей**, целью которого является дестабилизация политических отношений (в партиях, объединениях, движениях) для разжигания конфликтов и создания обстановки недоверия и подозрительности, формирования образа врага. Это распространение искаженной или заведомо ложной информации в пропагандистских, военных (введение противника в заблуждение) или других целях, а также предоставление ложной информации противнику [5, С. 12].

На сегодняшний день психологическое воздействие и дезинформация являются наиболее распространенными методами ведения информационной войны, которые встречаются повсеместно и необходимы для создания образа врага отдельных государств в глазах мировой общественности.

Искажение действительности в пропагандистских целях – традиционный прием информационной войны. Например, можно вспомнить широко растиражированные в США в 1990 году, накануне операции «Буря в пустыне, свидетельства 15-летней кувейтской девочки о том, как иракские солдаты разоряли кувейтские роддома. Впоследствии выяснилось, что девочка была дочерью кувейтского посла в США и не находилась в Кувейте в момент иракского вторжения, а ее свидетельства были инсценированы пиар-компанией, нанятой правительством Кувейта. Пропаганда всегда была особенно активна накануне и во время войн. Однако образ сегодня, благодаря прогрессу техники, обогнал по степени реальности факт, и факт стал вторичен, а образ первичен, даже в случае своего полного несоответствия фактам. Нужный образ делают ярким, а ненужный факт – неясным, дискуссионным или вообще несуществующим [8, С. 234].

Другим примером может служить Боснийская война 1992-1995 годов. Для того, что создать образ врага в роли Сербии, были проведены массовые информационные кампании. К примеру, начиная с 1992 года, западными СМИ постоянно публиковалась информация, которую выдавали за правду, зная, что это прямая ложь. Телевизионная компания США, которая носит название Independent Television Network, транслировала фотографии сербского «Лагеря смерти» [16, С. 23], где, как позже выяснилось, старик-босниец в традиционной сербской одежде рассказывал о жизни «за проволокой» [7, С. 11]. Необходимо было довести до общественности, что данный лагерь был создан сербами с целью издевательства над местными жителями. Спустя несколько лет лишь в 2008 году после обнародования достоверной информации выяснилось, что это был пункт (школа) для помощи сербским беженцам, бежавшим из Боснии. Натянутая проволока вокруг школьного двора пыталась уберечь детей от случайного выхода за территорию лагеря. Однако для Конгресса США данная дезинформация стала официальным поводом для американских законодателей занять и пропагандировать открытую антисербскую позицию во время боснийской войны. Им удалось заставить мир поверить в то, что они выступают в качестве защитника мусульман и ведут «гуманитарную войну». Постоянное разжигание антисербской истерии, искаженных фактов, необъективных цифр (то есть дезинформация) привело к силовому методу урегулирования конфликта и создании образа врага среди невинного населения [12, С. 148].

Примером **фальсификации** информации и распространения «фейковых новостей» может служить грузино-осетинский конфликт в 2008 году. Мировые СМИ начали внимательно следить за ходом конфликта после расположения российских миротворцев на территории Южной Осетии. Грузинское руководство с самого начала конфликта перестало транслировать российские телевизионные каналы, а веб-сайты с расширением .ru. было немедленно заблокированы. Заявления Грузии об осадном положении и наступлении войск РФ, о совершенных российскими солдатами «зверствах» (этнические чистки) над мирным населением, а также об обстреле некоторых грузинских городов вызвали резонанс среди мировой и российской общественности [9, С. 15].

Образ жертвы в лице Грузии сыграл важную роль в эскалации конфликта и распространении заранее подготовленной сфальсифицированной информации, благодаря которой западные СМИ расценивали Россию, как государство, вмешавшееся во внутригосударственный конфликт. Более того, по официальным данным американской газеты The Washington Post и британской The Times, у Грузии были многочисленные контракты с пиар-агентствами, которые описывали подробности, в несколько раз преувеличенные, хода военных действий [14, С. 145]. Благодаря американской поддержке, Грузия смогла осуществить несколько мероприятий с использованием фейк-новостей: это, прежде всего, образ агрессора со стороны РФ и вмешательство во внутренние дела Грузии; фальсификация хронологии событий; искажение действительной информации (завышали потери ВС); фальсифицирование фактов жестокого отношения российских миротворцев к местному грузинскому населению.

В роли третьего метода информационной войны многие ученые [15, С. 234] выделяют **«навязывание идеологии»** или **«информационно-идеологическую экспансии».**

Это воздействие на сознательные (подсознательные), политические и ценностные ориентации объектов (или же групп объектов) посредством распространения и навязывания взглядов, идей и учений с целью формирования мировоззрения, соответствующего интересам влияющей стороны.

Здесь важную роль играют социальные сети, медиаресурсы, чьи площадки можно использовать для распространения своих идей и навязывания их обществу разных

стран. Целевой аудиторией подобных медиа и телеканалов выступает молодежь, в умах которых формируются новые идеологические установки, выгодные для пропагандирующих их стран. К примеру, в США при Государственном Департаменте был создан Офис по вопросам цифрового взаимодействия, в обязанности рабочей группы которого входит взаимодействие с иностранной аудиторией и промывка мозгов.

Ярким примером может служить процесс глобализации и вестернизации, и, например, ситуация вокруг Китайской Республики (Тайвань). Решение об отделении от Китайской Народной Республики было принято еще в 1949 году, но окончательное оформление о его независимости приходится на конец 20-го века. Несмотря на то, что Китай не при каких обстоятельствах не признает независимость Тайваня, США активно вмешивается в решение данного вопроса, настраивая Тайваньское правительство против режима, господствующего на территории КНР. В 2008 году на выборах Президента Китайской Республики (Тайвань) американский Офис цифрового взаимодействия использовал всевозможные методы для вселения ссоры в отношения двух стран и обеспечения сотрудничества США и Тайваня через завоевание симпатий со стороны местных жителей [11, С. 170]. В массовые скопления людей были доставлены специальные американские газеты, в которых подробно описывались идеи американской демократии и ценностей их народа. Многие школы и университеты обучались по американским учебникам, где искаженная история Тайваня преподносится для молодежи с точки зрения разрешения конфликта с помощью демократизации и помощи США [2, С. 3–6]. Создание образа «спасителя» со стороны США, распространение идей американского народа, пропаганда собственной идеологии и образа жизни послужили неким толчком для переноса ценностных ориентиров на молодежь Тайваня, которые они охотно переняли и используют по сей день. Более 80% опрошенных Тайванцев считают, что внедрение демократии – это важный шаг на пути «к свободе», который может привести к военным столкновениям между Китаем и Тайванем.

Следующим методом выступает **«информационно-экономическая блокада» и «информационный империализм».**

Зависимость современного экономического сектора от информационных технологий побуждает правительства некоторых стран к ведению информационных экономических войн. Информационная блокада становится неуязвимым и эффективным методом, так как она носит скрытый характер и проникает в информационные сети (вместо ввода санкций или эмбарго) противника без возможности отслеживания. Наблюдается тенденция к обеспечению зависимости материальных поставок от непрерывной работы информационных потоков, поэтому стабильность экономического сектора зависит от доступа к информационным ресурсам.

Отличным примером глобализации информационных экономических рынков может служить международная телекоммуникационная банковская система SWIFT. С одной стороны, данная система очень надежна и обеспечивает работу только сертифицированных банков, а любой «нарушитель порядка» или попытка взлома грозит удалением из данной системы.

Главными плюсами данной системы являются: интеграция финансовых институтов различных стран в международную финансовую систему и оперативный способ получения и обмена экономически важной информацией. Однако данная система выступает в роли лица, управляющего мировой валютно-финансовой ситуацией, что можно наблюдать на примере «замораживания» иранских вкладов и невозможности иранских руководителей распоряжаться своими счетами, что впоследствии привело к обострению иранско-американских отношений.

Таким образом, исходя из вышесказанного, можно отметить, что информационная война не ограничивается кибератаками и хакерскими взломами. Данное понятие гораздо обширнее и представляет угрозу национальной безопасности государств.

Информационная война в контексте Российской Федерации

Сегодня Российская Федерация также рассматривает данную угрозу в качестве приоритетной. В общем виде, угрозы национальной безопасности России в информационной сфере представляют собой деятельность иностранных государств, террористических организаций и преступных группировок с целью вывода из строя российских информационных систем, нарушения суверенитета, территориальной целостности, изменения конституционного строя страны, невозможности реализации национальных интересов России, подрыва традиционных ценностей, основ жизни граждан, а также психологического воздействия.

Несмотря на многообразие методов ведения информационных войн, которые ранее упоминались в статье, необходимо отметить способы применения этих методов на практике и опасность, которую они представляют для системы национальной безопасности России:

Информационно-психологические угрозы – неверное истолкование концепций и стратегий и их внедрение в интеллектуальную среду страны с целью ослабления оборонного потенциала нации и вывода из строя системы государственного управления. Основными целями выступают: дестабилизация внутриполитической обстановки в стране; возможность прихода к власти прозападного режима; распространение идей о нелегитимности действующего Правительства; формирование протестных настроений среди российской общественности.

Например, 23 июня 2020 года Федеральное Агентство Новостей опубликовало отчет о финансировании Вашингтоном неправительственных организаций, находящихся на территории России и поддерживающих оппозиционные настроения. В число таких организаций вошли: движение «Солидарность», созданное в 2008 году при поддержке Бориса Немцова американскими спецслужбами; «За права человека» Льва Пономарева, «Голос», а также «Штабы» Алексея Навального, который активно проводил антиправительственную политику в 2020-2021 годах. Госдеп США проводил финансирование российской оппозиции (несколько сотен миллионов долларов) с помощью United States Agency for International Development («Агентство по международному развитию») через фонд National Endowment for Democracy («Национальный фонд демократии»), который ежегодно выделял более ста грантов на оппозиционные программы.

Информационно-когнитивные угрозы – воздействие на сознание населения, смены его мировоззрения, ценностей, манипулирование общественным мнением, и навязывание новой картины мира и мотивов поведения через средства массовой коммуникации, социальные сети, печатные и электронные издания. Основные цели: разрушение национальных ценностей и навязывание прозападных идеалов и моделей поведения; деструкция мировоззрения и миропонимания российской молодежи; кризис государственной идеологии, деформация системы норм и ценностей.

Угрозы демографическому суверенитету. Информационное воздействие неправительственных организаций оказывает прямое влияние на демографический по-

тенциал страны с целью подрыва демографических показателей России, а также: снижения численности населения; создания обстановки социальной напряженности в стране; развала традиционного института семьи и искоренения семейных ценностей; получения преимуществ западных стран в демографических показателях и сохранения конкурентоспособности в глобальном масштабе.

Используя средства массовой информации, площадки виртуального общения, рассылки, новостные паблики, социальные сети, а также тактические медиа, происходит информационная деятельность, направленная на нейтрализацию мужского начала у мужчин, подавление женского начала, создание конфликтности в отношении холостых людей и людей, уже состоящих в браке, на пропаганду однополых браков, что, в конечном итоге, приводит к расслоению населения на определенные группы и усиливает враждебные настроения между ними, которые влияют на рост или снижение уровня населения.

Угрозы территориальной целостности и суверенитету. Современные информационные войны, которые ведутся против России направлены на: вывод из строя российских информационных систем; реализацию возможности изменения конституционного строя страны; невозможность реализации национальных интересов России; распространение террористических организаций и преступных группировок на территории страны.

Российские инициативы по вопросам международной информационной безопасности (МИБ) в рамках ООН

Информационную безопасность принято рассматривать как наиболее важную часть осуществления внешней и внутренней политики любого государства, где наиболее важным элементом выступают национальные интересы, их реализация, охрана и продвижение на глобальном уровне.

Несмотря на то, что феномен проблематики МИБ существует достаточно давно, по-прежнему не существует единства мнений относительно терминологии в рассматриваемой сфере. В начале 1990-х годов, когда информационная безопасность стала объектом политологических работ, под ней понимали сферу отношений, противопоставленную информационной войне. Принципиальное отличие сущности современного понятия «информационная безопасность» и вкладываемого в него формального наполнения объясняется спецификой подхода к изучению МИБ, сложившегося почти два десятилетия назад.

Впервые в научно-аналитической литературе вопрос информационной безопасности (кибербезопасности) был затронут американским ученым Дж. Наем, автором концепции «мягкой силы» государства, в рамках работы «Будущее силы в XXI веке» [6, С. 20]. Най освещает беспрецедентное формирование новой концепции в международных отношениях – концепции киберсилы, смысл которой заключается в способности оказывать влияние на политическую, социальную и экономическую сферы международного сообщества через интернет-пространство.

Сегодня, когда вызовы глобальной информатизации становятся одной из главных проблем международной повестки дня, а информационное пространство и его террористическое осмысление – предметом ряда исследований, интерес российской общественности, политического сектора и представителей экспертного сообщества к проблематике МИБ неизменно растет. Как объект приложения интересов всех мировых акторов, МИБ способствовала формированию новой сферы, ставшей не только широким полем сотрудничества, но и источником новых противоречий.

Первой в мире страной, которая «забила тревогу» и начала выносить вопросы обеспечения ИБ на мировую площадку, была Россия. Наша страна – единственная в мире, которая самостоятельно разработала концепцию МИБ и выступила с ней в ООН. Дабы не углубляться в основные положения резолюции, важно отметить ее главные моменты – это предложение по контролю информационного оружия, равноправное владение этим оружием и невозможность применения оружия государствами друг против друга.

В свою очередь, представители российского экспертного сообщества смотрят на эту проблему гораздо шире, чем представители стран западного сообщества. Это отражается на эффективности российской внешней политики в данном направлении: в вопросах обеспечения МИБ Россия исходит из необходимости усиления контроля над Интернетом, демилитаризации информационного пространства, а также разработки определенных правил поведения в цифровой среде. Однако в то же время отсутствие согласованной позиции между Россией и Западом отдаляет перспективы введения единых принципов поведения.

Транснациональный характер информационного пространства определяет природу появляющихся в цифровой среде вызовов и угроз. В связи с этим проблема обеспечения режима МИБ и противодействия информационной преступности подчеркивает важность организации международного сотрудничества, учитывающего особенности информационного пространства и опирающегося на нормы международного права.

Как известно, Россия в течение многих лет указывала на необходимость взаимодействия и на сегодняшний день остается главным инициатором открытого диалога и продвижения норм и правил кибербезопасности, используя все существующие механизмы – от двусторонних переговоров с другими государствами и рассмотрения на полях различных форумов, таких как G20 и БРИКС, и до региональных интеграционных объединений и международных организаций.

Начиная с 1998 года, когда Россия впервые внесла на рассмотрение Генеральной Ассамблеи ООН проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной информационной безопасности», стало очевидно стремление российской стороны создать всеобъемлющие условия для формирования системы МИБ, а впоследствии – доказать всем участникам мирового сообщества, что угрозы в информационном пространстве сопоставимы по масштабу и последствиям с угрозами применения ядерного оружия. Неслучайно многие журналисты со всего мира нередко сравнивают проблему кибербезопасности с третьей мировой войной. Действительно, взаимодействие и равноправное стратегическое партнерство – это ключевое условие поддержания порядка и стабильности в цифровой среде. Информационная политика России и ее позиция по МИБ преследуют целью не развитие аналогичной противостоянию времен холодной войны системы международных отношений, а создание объединяющей площадки для практического сотрудничества и конструктивного открытого диалога.

Так, например, благодаря многолетним усилиям и активному участию России в вопросе обеспечения МИБ и мирного развития информационной среды, в ООН создается важный с дипломатической и политической точки зрения переговорный механизм – рабочая группа открытого состава (РГОС), пришедшая на смену ранее действовавшей Группы правительственных экспертов, которая прекратила свою работу ввиду ряда противоречий между участниками (США и их союзниками с одной стороны, и Россией, БРИКС и развивающимися странами – с другой). Несмотря на по-прежнему существующие разногласия, формирование РГОС – большой успех для российской

стороны, которая остается главным идеологом продвижения вопросов МИБ.

Россия неоднократно обращалась к государствам — членам ООН с вопросом о целесообразности создания международно-правового режима противодействия преступности с использованием ИКТ. С момента официальной постановки вопроса перед ООН российская резолюция по МИБ ежегодно принимается ГА ООН (в период с 1971 года по сегодняшний день их было принято более сорока, в частности последние «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» и «Противодействие использованию информационно-коммуникационных технологий в преступных целях»), а положения документа постоянно развиваются и дополняются идеями, отвечающими безопасности мирового сообщества.

Не стал исключением текст резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях», закрепивший принципиально важные положения об исключительно мирном использовании ИКТ, действие общепризнанных принципов международного права в информационном пространстве, обладание государственным суверенитетом над ИКТ-инфраструктурой на своей территории, запрет на ничем не подкрепленные обвинения в кибернападении и ряд других.

В этой связи стоит отметить и тот вклад, который Россия внесла в развитие терминологии ООН по МИБ. В ответ на революционные действия в ходе «арабской весны», когда социальные сети выступали инструментом обеспечения интересов и координации деятельности протестных режимов, Россия дополнила уже существующую так называемую «триаду угроз» новыми элементами, а именно: опасность вмешательства во внутренние дела суверенного государства посредством ИКТ, нарушение общественной стабильности и разжигание межэтнической, межнациональной розни. Тем не менее миротворческая киберконцепция России не соответствует позиции ряда государств во главе с США, которые опасаются потерять контроль и влияние в ИКТ-сфере и ограничить свои возможности, что в результате приводит к торможению процесса принятия и реализации российских инициатив по данному вопросу.

Заключение. Информационная война на сегодняшний день является актуальной и неотъемлемой составляющей международных отношений. Учитывая вовлеченность Российской Федерации в международные процессы, в том числе и конфликты, проблема информационных войн против России становится все более актуальной. Проанализировав на исторических примерах методы, механизмы ведения информационных войн, в том числе против России, невозможно переоценить важность внедрения новых и поддержку уже существующих практик и мер, способных в перспективе обеспечить информационную безопасность РФ и ее граждан. Сегодня проблема информационных войн уже приобрела глобальный характер, и полное ее разрешение возможно лишь усилиями всех участников мирового сообщества

Литература

1. Blakesley P. J. Shock and awe: A Widely Misunderstood Effect. United States Army Command and General Staff College, 2004.
2. Carter J. U.S. Course in a Changing World // Department of State Bulletin. 2008. V. 80. № 2038. P. 3–7.
3. Harlan K. Ullman, James P. Wade. Shock and Awe: Achieving Rapid Dominance. – Center for Advanced Concepts and Technology, For sale by the U.S. G.P.O., Superintendent of Documents, 1996. – 199 p.
4. Lazarsfeld R., Merton R.K. Mass Communication, Popular Taste, and Organized Social Action. New York IK college, 2004. – 17 p.
5. Linebarger P. M. A. Psychological warfare. United States Army Command and General Staff College, 2010.
6. Nye J.S. The Future of Power. New York: Public Affairs, 2010.
7. Schoen F. & Lamb Ch.J. Deception, Disinformation, and Strategic. Communications: How One Interagency Group. Washington, D.C.: National Defense University Press, 2012. 155 p.
8. Барабаш В.В., Бордюгов Г.А., Котеленец Е.А. Государственная пропаганда и информационные войны. Учебное пособие. – М.: АИРО-XXI, 2015. – 400 с.
9. Блиев М.М. Южная Осетия в коллизиях российско-грузинских отношений. М.: Европа, 2006. 468 с.
10. Гриняев С.Н. Информационная война в ходе агрессии США, Великобритании и их союзников против Ирака. Аналитический доклад. – Москва, 2010. – 118 с.
11. Гришин С.Е. Формирование культуры кибербезопасности в обществе – актуальная задача современности // Вестник Саратовского государственного социально-экономического университета. 2011. № 4 (38). С. 170– 173.
12. Засурский Я.Н. Техника дезинформации и обмана. М.: Мысль, 2010. 246 с.
13. Ламанова Е.В. Психологическая война: теория и практика обработки массового сознания. М.: Центрполиграф, 2013. – 667 с.
14. Михайленко Т.А. Особенности информационной войны в современном мире. На примере грузино-южноосетинского конфликта в августе 2008 года. Журнал Факультета государственного управления МГУ «Государственное управление. Электронный вестник», Выпуск № 19 (июнь 2009).
15. Новые вызовы и угрозы безопасности РФ в условиях глобальных и локальных трансформаций: монография / кол. авторов ; под общ. ред. С.В. Устинкина, А.В. Никитина. — Москва: РУСАЙНС, 2023. – 388 с.
16. Савинова А.А. Политический медиадискурс в эскалации этнического конфликта в Косово//Коммуникология: электронный научный журнал. Том 5. №1. С. 45-49.

Information warfare as a threat to the national security of the Russian Federation

Garaeva A.N., Kolobova S.A.

Linguistics University of Nizhny Novgorod

This article attempts to understand the concept of information warfare as a national security threat in Russia. In the context of current international events, the impact of the question of the principles and methods of waging information warfare is explored: propaganda, psychological warfare, disinformation, information and ideological expansion, information, cultural, and economic blockade, and cyberattacks. The author draws conclusions about the waning importance of this area of Russian security and the measures taken to counter information warfare and information security.

Keywords: information warfare, the Russian Federation, the USA, international information security, psychological influence, fake news, disinformation, propaganda.

References

1. Blakesley P. J. Shock and awe: A Widely Misunderstood Effect. United States Army Command and General Staff College, 2004.
2. Carter J. U.S. Course in a Changing World // Department of State Bulletin. 2008. V. 80. № 2038. P. 3–7.
3. Harlan K. Ullman, James P. Wade. Shock and Awe: Achieving Rapid Dominance. – Center for Advanced Concepts and Technology, For sale by the U.S. G.P.O., Superintendent of Documents, 1996. – 199 p.
4. Lazarsfeld R., Merton R.K. Mass Communication, Popular Taste, and Organized Social Action. New York IK college, 2004. – 17 p.
5. Linebarger P. M. A. Psychological warfare. United States Army Command and General Staff College, 2010.
6. Nye J.S. The Future of Power. New York: Public Affairs, 2010.
7. Schoen F. & Lamb Ch.J. Deception, Disinformation, and Strategic. Communications: How One Interagency Group. Washington, D.C.: National Defense University Press, 2012. 155 p.
8. Barabash V.V., Bordyugov G.A., Kotelenets E.A. State Propaganda and Information Wars. Study Guide. Moscow: AIRO-XXI, 2015, 400 p.
9. Bliev M.M. South Ossetia in Collisions of Russian-Georgian Relations. Moscow: Evropa, 2006, 468 p.

10. Grinyaev S.N. Information Warfare during the Aggression of the USA, Great Britain, and Their Allies against Iraq. Analytical Report. Moscow, 2010, 118 p.
11. Grishin S.E. Formation of a Culture of Cybersecurity in Society – a Urgent Task of Our Time // Bulletin of the Saratov State Socio-Economic University. 2011, No. 4 (38). P. 170–173.
12. Zasursky Ya.N. Techniques of Disinformation and Deception. Moscow: Mysl', 2010. 246 p.
13. Lamanova E.V. Psychological Warfare: Theory and Practice of Processing Mass Consciousness. Moscow: Tsentrpoligraf, 2013. – 667 p.
14. Mikhayilenko T.A. Features of Information Warfare in the Modern World. On the Example of the Georgian-South Ossetian Conflict in August 2008. Journal of the Faculty of Public Administration, Moscow State University "Public Administration. Electronic Bulletin", Issue No. 19 (June 2009).
15. New Challenges and Threats to Russian Federation Security in the Context of Global and Local Transformations: monograph / collective of authors; under the general editorship of S.V. Ustinkin, A.V. Nikitin. — Moscow: RUSAINS, 2023. – 388 p.
16. Savinova A.A. Political media discourse in the escalation of the ethnic conflict in Kosovo//Communicology: electronic scientific journal. Vol. 5. No. 1. Pp. 45-49.