ИНФОРМАЦИОННЫЕ ВОЙНЫ № 4(52) 2019

Научно-практический междисциплинарный журнал

Теория войн, информационное противоборство, информационный менеджмент, управление конфликтами и рисками, информационная безопасность, образование, математическая психология, вопросы истории.

Группа специальностей: политология (23.00.00).
Политические, социологические науки.

РОССИЙСКАЯ АКАДЕМИЯ НАУК
ЦЕНТР ИССЛЕДОВАНИЙ ПРОБЛЕМ БЕЗОПАСНОСТИ

АКАДЕМИЯ ВОЕННЫХ НАУК
ЦЕНТР ПРОБЛЕМ СТРАТЕГИЧЕСКИХ ЯДЕРНЫХ СИЛ

Издается с апреля 2007 г.
Свидетельство о регистрации
ПИ № ФС77-28172
от 28 апреля 2007г.

ISSN 1996-4544

Выходит 4 раза в год

СОДЕРЖАНИЕ

Журнал включен в «Перечень ведущих периодических изданий» ВАК.

I. ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО АКТУАЛЬНЫЕ ПРОБЛЕМЫ. ТЕОРИЯ

УДК 32.019.5

© Лепский В.Е.

© Lepskiy V.

ПРОБЛЕМА СБОРКИ СУБЪЕКТОВ В ИНФОРМАЦИОННЫХ ВОЙНАХ

THE PROBLEM OF ASSEMBLY OF SUBJECTS IN INFORMATION WARS

Аннотация. *Обосновывается актуальность проблемы сборки субъектов в информационных войнах. Предлагается структура параметров сборки субъектов. На основе предложенных параметров анализируется смена оснований сборки субъектов Североатлантического блока, превращающего его в культовую организацию. В контексте сборки субъектов анализируется концепция управляемой конфронтации, которая представляется как сборка «виртуального субъекта». Обосновывается актуальность этой концепции в условиях перехода от однополярного к многополярному миру. На примере технологии управляемого хаоса анализируются возможности разрушения (разборки) субъектов в информационных войнах. Предлагается российский асимметричный ответ информационным войнам как организация сборки субъектов мирового развития. Реализация этой миссии представляется как решение проблемы перехода от техногенной к социогуманитарной цивилизации, для которой у России имеется адекватный исторический опыт и культурные основания, а также современный научный задел кибернетики саморазвивающихся полисубъектных (рефлексивно-активных) сред, опирающийся на философские основания постнеклассической научной рациональности.*

Работа выполнена при финансовой поддержке РФФИ (проекты №18-011-00567 и №18-511-00008-Бел_а).

Abstract. *The article substantiates the urgency of the problem of assembly of the subjects in information wars. The structure of the parameters of assembly of the subjects is proposed. The paper contains an analysis of the change of bases for assembly the subjects of the North Atlantic bloc, which turns it into a cult organization. In the context of the assembly of the subjects, the concept of guided confrontation is analyzed, which is presented as an assembly of the "virtual subject". The relevance of this concept in the transition from a unipolar to a multipolar world is substantiated. Using the example of controlled chaos technology, the possibilities of destruction (disassembly) of subjects in information wars are analyzed. The Russian asymmetric response to information wars is proposed as an organization for assembling the subjects of world development. Realization of this mission is presented as a solution to the problem of transition from a technogenic to a socio-humanitarian civilization, for which Russia has adequate historical experience and cultural foundations, as well as a modern scientific background of the cybernetics of self-developing polysubject (reflexive-active) environments based on the philosophical foundations of post-non-classical scientific rationality.*

This work was supported by the Russian Foundation for Basic Research (projects No. 18-011-00567 and No. 18-511-00008-Bel_a).

Ключевые слова. *Сборка субъектов, информационная война, саморазвивающаясяся рефлексивно-активная среда, рефлексивная технология, постнеклассическая рациональность.*

Key words. *Assembly of subjects, information war, self-developing reflective-active environment, reflective technology, post-non-classical rationality.*

1. Введение

Нарастающие масштабы и сложность гибридных войн требует создания современных адекватных механизмов защиты от информационных угроз, организации активных форм противодействия и нейтрализации последствий. Анализ проведенных и проводимых в последние десятилетие информационных операций против России позволяет сделать вывод о недостаточной согласованности действий представителей государства, бизнеса и общества, об отсутствии успешной консолидации их усилий в интересах обеспечения национальной безопасности и развития страны.

Можно назвать много причин сложившейся ситуации: отсутствие доверия в треугольники «государство − бизнес − общество»; гигантское расслоение общества на бедных и богатых; отсутствие равенства перед законом; нарушение Конституции Российской Федерации по статьям, связанным с социальным государством и властными полномочиями народа; отсутствие идеологии и образа будущей России и др. Как следствие, диагноз − «бессубъектность российского развития» [1]. Этот диагноз не позволит обеспечить эффективную защиту страны от угроз гибридных и информационных войн в XXI веке.

Центральной проблемой становится проблема сборки субъектов в интересах обеспечения национальной безопасности и развития страны [2].

В статье представлена обобщенная структура параметров сборки субъектов. Рассмотрены типовые технологии сборки субъектов в информационных войнах. Предложена технология управляемой конфронтации для сборки виртуальных субъектов в информационных войнах, актуальность которой возрастает в связи с трендом перехода от однополярного к мно-

Лепский Владимир Евгеньевич *– доктор психологических наук, главный научный сотрудник, Институт философии РАН, тел. +7(916)-634-76-52.*

Lepskiy Vladimir *– doctor of psychological sciences, leading research fellow, Institute of Philosophy of the Russian Academy of Sciences, tel. +7 916-634-76-52.*

гополярному миру. Приведен пример «успешно» используемой в гибридных войнах технологии управляемого хаоса для разрушения субъектности развития. Предложена модель сборки субъектов развития в саморазвивающихся рефлексивно-активных средах (кибернетика третьего порядка), рассматриваемая как асимметричный ответ современным информационным войнам.

2. Параметры сборки субъектов

Понятие «сборка субъектов» новое и введено нами [3] для объединения разнородных представлений и технологий соорганизации субъектов в целостного совокупного субъекта. Эта проблема рассматривалась в различных областях научного знания (философии, психологии, социологии, экономике, политологии, кибернетике, синергетике и др.). Накоплен богатый опыт практических приложений: политических, экономических, этнических и других социальных процессов, культовых организаций, формирования разнообразных видов команд для выполнения общих задач (космос, военные системы, бизнес, спорт и др.), а также во многих других сферах человеческой деятельности. Что дает основания утверждать об актуальности четкой постановки и решения проблемы сборки субъектов развития в междисциплинарном контексте.

Принципиально важно отметить, что ключевые параметры, которые лягут в основу процессов сборки субъектов развития определяют образ будущего коллективного субъекта. Нами предложен вариант структуры параметров сборки субъектов в контексте рассмотрения от классической к постнеклассической научной рациональности. Этот вариант является первой попыткой на пути систематизации параметров сборки субъектов и должен рассматриваться как «пилотный» вариант и фактически фрагмент структуры подлежащей развитию [2].

Уточним отдельные используемые понятия.

Совокупный субъект – субъект, образующийся в результате процессов сборки субъектов.

Базовые субъекты – субъекты, которые собираются в совокупного субъекта.

Параметры сборки субъектов – один из инструментов понижения размерности (сложности) системы сборки субъектов. Это коллективная переменная функция многих входящих в нее других переменных, в анализе сложных самоорганизующихся систем сборки субъектов, дающая важную информацию о поведении последних как сложно структурированных целостностей. Будем выделять две группы параметров сборки субъектов: базовые основания для сборки субъектов и базовые факторы, влияющие на процессы сборки субъектов.

Базовые основания для сборки субъектов – это те основания, которые определяют ведущие мотивы субъектов в их ориентации на процессы сборки. Среди такого рода оснований в первую очередь следует выделить: общность ценностей, общность культуры, общность целей, а также комплексные основания, формируемые, например, в процессах «проектной идентификации».

Базовые факторы, влияющие на процессы сборки субъектов – это факторы (группы факторов) наиболее значимые для процессов сборки субъектов, влияние которых изучено в различных областях знания.

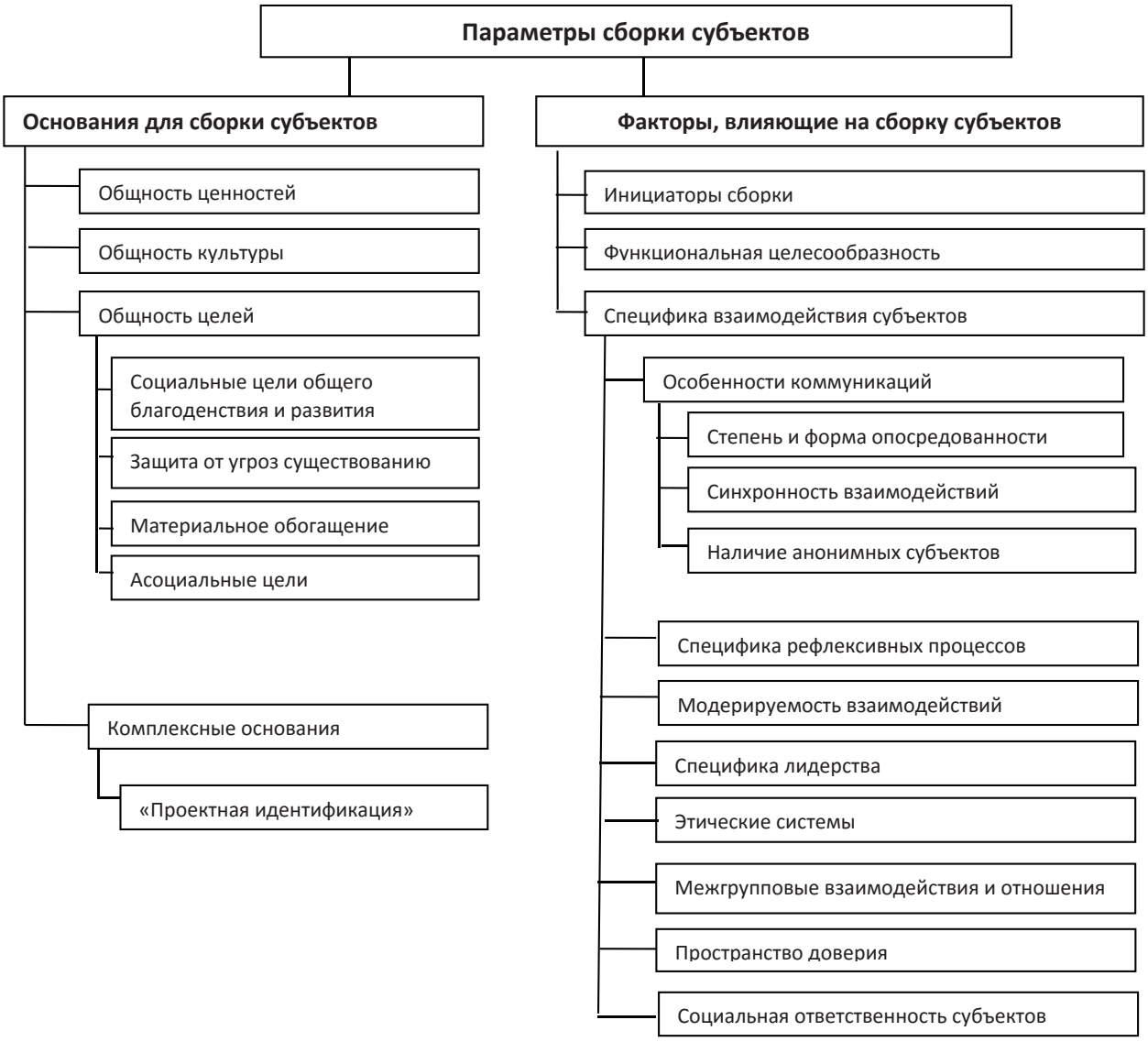
Проведенный нами предварительный анализ позволил выделить следующую структуру параметров сборки субъектов (см.рисунок). Предлагая данную структуру, мы понимаем, что она открыта для коррекции и дальнейшего развития. На наш взгляд, она может быть полезна как для постановки новых исследовательских задач, так и для практической работы. Анализ специфики приведенных параметров сборки субъектов и их влияние на совокупного субъекта представлен в монографии [2].

Среди выделенных в структуре базовых оснований для сборки субъектов многие параметры являлись и являются предметом исследований в различных областях научного знания. Например, ценностно-ориентационному единству при формировании групповых субъектов посвящены многочисленные исследования в социальной психологии. Общность культурных и целевых оснований имеет богатый опыт исследований в социологии. Нам представляется наиболее значимым для современной России и в то же время наименее изученным комплексное основание – «проектная идентификация». Она органично вписывается в представления о постнеклассической научной рациональности и может быть успешно реализована в саморазвивающихся полисубъектных (рефлексивно-активных) средах [4].

3. Смена оснований сборки субъектов Североатлантического блока, превращающего его в культовую организацию

Североатлантический блок был основан в 1949 г. с целью защиты его членов от возможных угроз со стороны СССР и его союзников. В условиях противостояния двух идеологий и нарастающих военных угроз образование этого блока опиралось на общность целей участников «защита от угроз существованию». Это основание было понятным всем участникам и способствовало сборке субъектов блока до момента развала СССР. После развала СССР это основание потеряло логическое обоснование, но тем не менее постоянно со стороны лидера блока внушалось членам блока его существование. На самом деле лидер блока решал свою задачу становления и поддержания однополярного мироустройства, в котором большей части человечества отводится роль обслуживания избранных на основе неэквивалентного экономического обмена.

Для решения этой задачи сохранение Североатлантического блока было полезно, но для сборки субъектов блока в новых условиях потребовалось использование новых соответствующих параметров сборки. Базовым основанием явились асоциальные цели, эгоистического отношения к большей части человечества. Естественно, такие цели официально нельзя было представлять человечеству, относя лидера и участников блока к цивилизованным странам. Поэтому официально декларировалась старая цель «защита от угроз существованию», которая была явно надu-



Фрагмент структуры параметров сборки субъектов

манной и лицемерной.

Участники блока, безусловно, понимали смену оснований сборки субъектов блока, но надеялись, что они попадают в круг избранных и их ожидают будущие привилегии. Кроме того, лидер блока дополнительно стал использовать ряд факторов, влияющих на сборку субъектов для предотвращения возможных возмущений со стороны участников, среди которых имеющие непосредственное отношение к сборке субъектов в культовых организациях (тоталитарных сектах) [5].

Главной целью любой тоталитарной секты является навязывание ее членам формы жизнедеятельности, считающейся нормой для последователей определенного культа. В технологическом аспекте ключевыми оказываются рефлексивные технологии воздействия на членов организации. Рассмотрим базовые рефлексивные технологии, реализуемые в контексте схемы управления формой жизнедеятельности в сектах.

В психологии выделяется два способа существования человека как субъекта жизни (жизнедеятельности) [6]. Первый – жизнь, не выходящая за пределы непосредственных связей, в которых живет человек (его можно назвать “реактивный” способ существования). Второй связан с актуализацией рефлексии. Сознание выступает как разрыв, как выход из полной поглощенности непосредственным процессом жизни для выработки соответствующего отношения к ней, занятия позиции над ней, вне ее для суждения о ней («рефлексивный» способ существования).

В тоталитарных организациях используются технологии, ориентированные на формирование “реактивного» способа существования ее членов. Обобщенно комплекс таких технологий можно назвать «Схема рефлексивного программирования», которая в общих чертах включает следующие процедуры:

• «разрыв ранее сложившейся жизнедеятельности». Ситуация после развала СССР;

• «рефлексивная блокада» – блокировка «несанкционированных» лидером блока рефлексивных процессов, фактически лишение субъектов возможности самостоятельно осуществлять осознанное создание или выбор новой формы жизнедеятельности. Прежде всего это «блокировка рефлексии» участников. Лидер блока без должных обоснований в силу своего доминирующего влияния на участников втягивает их в боевые действия в Югославии, Афганистане, Ливии, Сирии и др. Это явно не соответствует декларируемой ранее цели сбор-

ки субъектов «защита от угроз существованию»;

• «социальная изоляция» – блокировка «несанкционированных» лидером блока информационно-психологических воздействий социального окружения, фактически лишение возможности влияния на процессы создания или выбора новой формы жизнедеятельности ближайшего социального окружения субъектов. Иллюстрацией таких воздействий может служить организованная «технология санкций», устанавливаемая лидером блока, к которой должны без обоснований присоединиться участники блока в ущерб своим интересам и с разрушением связей с другими субъектами;

• «рефлексивное программирование» – навязывание заранее предопределенных лидером блока представлений, точек зрения, позиций, мнений и других психических образований с целью сформировать осознанное принятие предлагаемой нормы жизнедеятельности. Иллюстрацией является навязывание лидером блока участникам своих представлений об образе лидера как идеале будущего мироустройства, негативном образе отдельных субъектов («Россия агрессор»), скрытом перехвате государственного управления (на Украине, в Грузии и др.).

При использовании «Схемы рефлексивного программирования» субъект (участник блока) превращается в объект управления. Процедуры «Рефлексивной блокады», «Социальной изоляции» и «Рефлексивного программирования» способствуют закреплению «реактивного способа жизнедеятельности» и никоим образом не способствуют развитию субъектов. Эти процедуры явно ограничивают свободу субъектов, что отчетливо проявляется в последние годы в поведение ряда европейских стран, участников блока.

Более того, в последние годы приходит осознание, что участники блока не попадают в круг избранных, и не являются партнерами лидера, ибо все чаще за их счет начинают реализовываться национальные интересы лидера (поддержка рядом европейских стран проекта «Северный поток-2», частичный выход Турции из-под контроля лидера блока и др.).

Приведенные соображения убедительно доказывают, что в Североатлантическом блоке в последние тридцать лет произошла смена оснований сборки субъектов, что привело к перерождению этого блока в тоталитарную культовую организацию.

4. Технология управляемой конфронтации для сборки виртуальных субъектов в информационных войнах

В реалиях международных отношений иногда возникают ситуации, когда конфликтующим субъектам бывает выгодно временно «закрыть глаза на свои конфликты» и объединить усилия для предотвращения более глобальных угроз. Например, когда возникают угрозы глобального терроризма или возникают угрозы применения каким-либо субъектом оружия массового поражения. Для таких ситуаций В.А. Лефевр предложил концепцию управляемой конфронтации [7].

Суть этой концепции в скрытом объединении двух (или более) субъектов политической деятельности для организации скрытой совместной деятельности при возникновении внешних угроз, более значимых, чем угрозы в их взаимодействиях. При этом они заранее готовят реальные скрытые оперативные механизмы организации совместного взаимодействия в случае возникновения более значимых для них внешних угроз. Для внешних субъектов они находятся в конфликте и рассматриваются как автономные субъекты. На самом деле ситуация принципиально меняется, происходит процесс сборки нового совокупного субъекта, который оказывается «невидимым» для других субъектов и более могущественным, чем каждый из входящих в его состав субъектов. Такого рода процесс сборки субъектов мы назвали эффектом «виртуального субъекта», результатом сборки является «виртуальный субъект». Возникновение «виртуального субъекта» принципиально меняет ситуацию информационного противодействия. Резко повышается сложность организации информационных воздействий на «виртуального субъекта» и включенных в его состав субъектов, и соответственно повышается их информационная безопасность.

Возникновение «виртуального субъекта» меняет характер рефлексивных процессов в конфликтных взаимодействиях. Нарушается адекватность рефлексивных моделей внешних субъектов, они не отражают возникновение «виртуального субъекта» и, как следствие, для них возникают угрозы стать жертвой рефлексивного управления. Для внешних субъектов становится крайне затруднительным прогнозирование принятия решений субъектами, входящими в состав «виртуального субъекта», поскольку процессы принятия решений принципиально изменяются после их сборки в совокупного субъекта.

Эффект «виртуального субъекта» был исследован нами в экспериментах с межгрупповыми конфликтными взаимодействиями. Было обнаружено, что игрок, выигрывающий во взаимодействиях «один на один» у всех других участников игр, проигрывает во взаимодействиях «один против двоих», более слабых игроков [8]. Это было связано со сборкой слабых игроков в «виртуального субъекта», которого не мог адекватно моделировать сильный игрок. Важно заметить, что существенным фактором оказался тип лидерства в групповых отношениях. Эти исследования оказали также влияние на смену методик отбора команд (экипажей) для выполнения сложных групповых заданий.

Инициативно в начале 2000 годов нами была разработана модель организации управляемой конфронтации «Россия – США», ориентированная на создание оперативных механизмов скрытого объединения наших усилий в борьбе с зарождающимися мировыми террористическими организациями. Реакция со стороны США была не однозначна: представители Пентагоновских структур были «за», а Государственный департамент США уже не видел Россию как стратегического партнера или противника. Со стороны России не было проявлено интереса к этим предложениям в структурах, ответственных на национальную безопасность страны. Если бы тогда удалось организовать управляемую конфронтацию «Россия – США»,

то удалось бы избежать многих кровопролитных процессов.

Сегодня Россия другая и, возможно, имеет смысл вернуться к этим технологиям с субъектами, стремящимися к гармонизации мирового сообщества. Актуальность этой технологии повышается также в связи с переходом от однополярного к многополярному миру, она позволит «мягко» уйти отдельным субъектам от чрезмерной опеки лидера однополярного мира. А лидеру однополярного мира эта технология позволит «не потерять лицо» и найти достойное место в новом мироустройстве.

5. Технология управляемого хаоса для разрушения субъектов в информационных войнах

Альтернативой сборки субъектов в информационных войнах является их разрушение (разборка). Примером наиболее отработанной и распространенной технологией разборки субъектов в гибридных войнах является технология управляемого хаоса [9]. Эта технология может быть отнесена к оружию массового поражения, неконтролируемого в настоящее время международными организациями.

Эта технология была применена и к России для разрушения субъектности ее развития. В значительной степени под ее влиянием была сформирована бессубъектность российского развития [10].

Технология управляемого хаоса была ориентирована на разрушение базовых качеств субъектности развития (целеустремленность, рефлексия, коммуникативность, свобода влияния на события в стране, способность к развитию). Для этого был использован комплекс из десятков технологий, в результате воздействия которых был достигнут желаемый результат – бессубъектность российского развития. Одновременно с этим были созданы благоприятные условия для создания «ручной властной элиты» и формирования новой организованности для внешнего управления [9].

Организация бессубъектности российского развития сказалась и на ее бессубъектности в информационных войнах, что отчетливо проявилось в недостаточной эффективности противодействия информационной агрессии против нашей страны. Для эффективной организации информационного противоборства надо знать стратегические ориентиры развития страны, ее образ будущего, а с этим большая проблема, в стране фактически отсутствуют механизмы стратегического целеполагания [11].

Использование технологий управляемого хаоса явно противоречит принятым международным нормам о невмешательстве во внутренние дела государств. Эти аргументы дают основания для постановки проблемы запрета и организации международного контроля над использованием технологий управляемого хаоса. Россия в последние десятилетия была активным инициатором правового регулирования в сфере международной информационной безопасности, сегодня она могла бы выступить также инициатором в сфере международного правового регулирования использования технологий управляемого хаоса.

6. Сборка субъектов мирового развития как российский асимметричный ответ информационным войнам XXI века

Интенсификация информационных войн в начале XXI века убедительно продемонстрировала, что экономические и политические механизмы, опирающиеся на концептуальные основы капитализма и «жесткой» глобализации, являются угрозой для будущего человечества. Затянувшаяся борьба с радикальным исламизмом также продемонстрировала, что экономическими и военными воздействиями победить его проблематично. Для гармонизации мирового сообщества и, как следствие, снижения напряженности информационных войн необходим поиск адекватных сложившейся ситуации форм жизнедеятельности, под которые должны быть созданы адекватные им экономические механизмы.

Процесс социальной эволюции на нашей планете подошел к критической фазе макросдвига, когда трансформация общества достигает критического порога. Общество вступает в период социального и культурного хаоса. Человечество подошло к своего роду метасистемному цивилизационному переходу. Мировое сообщество не осознает целей и возможностей своего развития, не берет в должной степени ответственности за свои же деяния перед жителями планеты и различными социокультурными образованиями, перед природой и мирозданием в целом. "Бессубъектность развития" – главная болезнь мирового сообщества и главная причина нарастающих информационных войн. Как следствие, актуальна проблема сборки субъектов мирового развития. Решение этой проблемы может стать асимметричным ответом информационным войнам XXI века.

Проблема становления субъектности развития человечества неразрывно связана с поиском новых моделей цивилизационного развития. В настоящее время на планете доминирует техногенная модель цивилизационного развития (техногенная цивилизация), инициатором и творцом которой явилась западная цивилизация. Техногенная цивилизация опирается на принцип максимизации прибыли, на эгоизм субъектов рыночной экономики, на общество потребления. Эти основания не позволят организовать сборку субъектов мирового развития. В основу цивилизационной модели будущего должны быть положены другие базовые ценности, позволяющие преодолеть эгоизм разнообразных типов субъектности. К высшему уровню таких ценностей могут быть отнесены: сохранение и развитие человека; сохранение и развитие человечества; сохранение и развитие биосферы; сохранение и развитие техносферы, в которой всё большую роль играет цифровая реальность [12]. Эти ценности образуют систему взаимосвязанных ценностей, на которые нужно ориентироваться при целеполагании, понимая их взаимосвязи. Именно такие ценности могут позволить попытаться преодолеть рыночный эгоизм в масштабах человечества и попытаться найти адекватные модели жизнедеятельности.

Фактически речь идет о планетарном цивилизационном переходе от техногенной к социогуманитарной

цивилизации, к цивилизации гармонии субъектов развития. При переходе к социогуманитарной цивилизации человечество сможет сформировать субъектность своего развития. Этот цивилизационный переход неизбежен, ибо в противном случае человечество будет нарастающими темпами приближаться к катастрофе. Как следствие, встает проблема преодоления стихийной, неконтролируемой человечеством техногенной возгонки по технологическим укладам через переход в VII социогуманитарный технологический уклад [13], с позиций которого будет происходить управление предыдущими и будущими техногенными укладами в интересах развития человечества.

Кто станет лидером цивилизационного перехода? Россия имеет этот шанс в силу своего уникального исторического опыта и культурных оснований, позволяющих гармонизировать межэтнические, межконфессиональные, межцивилизационные отношения и обеспечивать развитие на больших временных интервалах. Для России такая миссия особенно актуальна, поскольку догнать развитые страны на технократическом пути развития безнадежно, более того к настоящему времени разрыв только увеличивается. Надо не догонять, а опередить и стать лидером технологий следующего поколения.

Философско-методологическими основаниями могли бы стать идеи постнеклассической научной рациональности (академик В.С. Степин) [14]. Постнеклассическая научная рациональность задает четыре важнейших основания для гармонии субъектов мирового развития. Во-первых, методологически обоснованное совместное представление субъектов, средств и объектов в процессах познания и деятельностной активности. Во-вторых, включение в процессы познания социальных ценностей и целей наряду с внутринаучными ценностями. В-третьих, введение в научную и управленческую деятельность этических регуляторов и принципиально важных связей с культурой. В-четвертых, задание постнеклассической рациональности не только как специфического вида рациональности, но и как рамочной методологической конструкции, органично включающей классическую и неклассическую рациональности.

В соответствие с логикой постнеклассической научной рациональности механизм развития представляется как саморазвивающаяся полисубъектная (рефлексивно-активная) среда [4].

В настоящее время имеется отечественный научно-методический задел для организации саморазвивающихся полисубъектных сред, который можно относительно быстро развить до использования в пилотных проектах. Интегратором научного обеспечения может выступить создаваемая в настоящее время постнеклассическая кибернетика саморазвивающихся полисубъектных сред. Это социогуманитарная кибернетика третьего порядка [15], создаваемая в логике восхождения от кибернетики «наблюдаемых систем» (первого порядка – Н. Винер) – классическая научная рациональность, к кибернетике «наблюдающих систем» (второго порядка – Фон Ферстер) – неклассическая научная рациональность и далее к социогуманитарной кибернетике «саморазвивающихся рефлексивно-активных сред» (третьего порядка) - постнеклассическая научная рациональность. Уточнение сходства и различия философских оснований видения кибернетики будущего на Западе и в России было проведено на мировом конгрессе WOSC2017 в январе 2017 г. в Риме и на XI международном симпозиуме «Рефлексивные процессы и управление» в октябре 2017 г. в Москве. В международном научном сообществе одобрены предложенные нами идеи кибернетики третьего порядка и намечены пути дальнейшего сотрудничества [16]. Есть основания полагать, что кибернетика третьего порядка могла бы стать научным обеспечением перехода от техногенной к социогуманитарной цивилизации, перехода к VII социогуманитарному технологическому укладу.

Предлагаемый подход можно рассматривать как российский асимметричный ответ информационным войнам XXI века. Он создает предпосылки для становления России планетарным лидером социальных преобразований, лидером сборки субъектов мирового развития, создает возможности для интенсивного и безопасного развития России и мирового сообщества.

7. Заключение

Обоснована актуальность проблемы сборки субъектов в информационных войнах. Поставлена междисциплинарная проблема сборки субъектов и предложена структура параметров организации сборки субъектов. На примере Североатлантического блока показана смена оснований сборки субъектов, которая привела к трансформации блока в тоталитарную культовую организацию. В контексте проблемы сборки субъектов проанализирована концепция управляемой конфронтации, в которой ключевой оказалась технология сборки «виртуального субъекта». Обосновано повышение актуальности концепции управляемой конфронтации в условиях перехода от однополярного к многополярному миру. Рассмотрен пример разборки субъектов на основе технологии управляемого хаоса. На основе проведенного исследования предложен для России асимметричный ответ информационным войнам через организацию сборки субъектов мирового развития, через организацию перехода от техногенной к социогуманитарной цивилизации.

Литература

1. Лепский В.Е. Методологический и философский анализ развития проблематики управления. – М.: Когито-Центр, 2019. – 340 с. URL: http://www.reflexion.ru/Library/Lepskiy2019.pdf.

2. Лепский В.Е. Аналитика сборки субъектов развития – М.: Когито-Центр, 2016. – 130 с. URL:http://www.reflexion.ru/Library/Lepskiy2016.pdf.

3. Лепский В.Е. Эскиз структуры параметров сборки субъектов и их дескриптивной модели // Проблема сборки субъектов в постнеклассической науке / Под ред. В.И.Аршинова, В.Е.Лепского. – М.: Издательство Института

философии РАН. 2010. − С. 185-217.
4. Лепский В.Е. Рефлексивно-активные среды инновационного развития. – М.: Изд-во «Когито-Центр», 2010. – 255 с. URL:http://www.reflexion.ru/Library/Lepsky_2010a.pdf.
5. Лепский В.Е., Степанов А.М. Особенности рефлексивных процессов в культовых организациях // Рефлексивные процессы и управление. 2002. N2. С. 59-72. URL:http://www.reflexion.ru/Library/J2002_2.pdf.
6. Рубинштейн С.Л. Человек и мир /Проблемы общей психологии.− М.: Педагогика, 1976. − С.253-381.
7. Лефевр В.А. Просчеты миротворчества. // Рефлексивные процессы и управление.− 2002, № 2. − С. 48-51.
8. Лепский В.Е. Концепция субъектно-ориентированной компьютеризации управленческой деятельности. − М.: Институт психологии РАН, 1998. − 204с.
9. Лепский В.Е. Технологии управляемого хаоса – оружие разрушения субъектности развития // Информационные войны. − 2010, N4. −С.69-78, URL:http://www.reflexion.ru/Library/Lepsky_2010.pdf.
10. Ипполитов К.Х., Лепский В.Е. О стратегических ориентирах развития России: что делать и куда идти // Рефлексивные процессы и управление. − 2003, том 3. № 1. − С.5-27. URL:http://www.reflexion.ru/Library/Ippol_2003.htm
11. Лепский В.Е. Стратегическое целеполагание в России: состояние и перспективы развития // Труды Вольного экономического общества России. − 2019, том 215, № 1. − С. 66-80. URL:http://www.veorus.ru/upload/iblock/657/veo_215.pdf.
12. Иванов В.В., Малинецкий Г.Г. Цифровая экономика: мифы, реальность, перспектива.− М.: Российская академия наук, 2017. — 64 с.
13. Лепский В.Е. Седьмой социогуманитарный технологический уклад – адекватный ответ технологическим вызовам XXI века / Философия в диалоге культур: материалы Всемирного дня философии. – М.: Прогресс-Традиция, 2010. − С. 1010-1021.
14. Степин В.С. Теоретическое знание. − М.: Прогресс-Традиция, 2003. – 744 с.
15. Vladimir Lepskiy. Evolution of cybernetics: philosophical and methodological analysis. Kybernetes, 2018, Vol. 47. Issue: 2, pp. 249-261. URL:https://doi.org/10.1108/K-03-2017-0120.
16. Stuart A. Umpleby, Tatiana A. Medvedeva & Vladimir Lepskiy. Recent Developments in Cybernetics, from Cognition to Social Systems. Cybernetics and Systems. 2019, Volume 50, Issue 4, pp. 367-382. URL:https://doi.org/10.1080/01969722.2019.1574326.

Материал поступил в редакцию 20.09.2019 г.

УДК 32.019.5

© Григорьев В.Р., Ковалев В.И.

© Grigoryev V., Kovalev V.

«НОВАЯ» СТРАТЕГИЯ США ПО СДЕРЖИВАНИЮ/ИЗМАТЫВАНИЮ РОССИИ В РАМКАХ КОНЦЕПЦИИ «ПРЕЭМПТИВНОЙ ВОЙНЫ»

«NEW» US STRATEGY TO CONTAIN / EXHAUST RUSSIA IN THE FRAMEWORK OF THE CONCEPT OF «PRE-EMPTIVE WAR»

Аннотация. *В статье проведен анализ предложений корпорации РЭНД по так называемой новой стратегии сдерживания/изматывания, а по сути, развала России посредством ее последовательного и «неминуемого» перенапряжения и изнурения, выраженных в последовавших за последние несколько месяцев друг за другом трёх докладах. Показано, что по сути, речь идёт об отработанных и по развалу СССР и ряду других государств стратегий рефлексивного управления, роевого воздействия сетецентрических инструментов ведения «гибридной войны» и «управляемого хаоса» путем точечного «аккупунктурного» воздействия на «болевые» точки РФ («точки уязвимости»), когда регулярные и синхронизированные воздействия в окрестности точки бифуркации (перехода сложной макроэкономической системы в новое качество устойчивости или неустойчивости/дестабилизации) должны позволить гарантированно разрушить макроэкономическую и внутриполитическую устойчивость российского государства, т.е. добиться результата без непосредственного применения военной силы, при этом демонстрируя разящий «силовой трезубец НАТО», размещая в соседних с РФ государствах новые воинские контингенты и системы наступательного вооружения, по сути, приближая НАТО к Москве на расстояние «пистолетного выстрела» при взведенном курке.*

Выявлены новые угрозы безопасности России, связанные с возможной реализацией данных предложений. Для их нейтрализации предложено проведение объективного упреждающего анализа, позволяющего выявить угрозу социально-политической дестабилизации России на ранней ее стадии и выработать своевременные меры по парированию этой угрозы. Показано, что методики анализа должны позволять реализовать систему постоянно действующего мониторинга степени данной угрозы в наиболее важных для России странах и систему поддержки принятия решений в области обеспечения социально-политической устойчивости общества.

Работа выполнена при поддержке РФФИ (проект 18-011-00567).

Abstract. *The article analyzes the proposals of the RAND Corporation for the so-called new strategy of containment / exhaustion, and, in fact, the collapse of Russia through its consistent and "inevitable" overstrain and exhaustion, expressed in three reports following the last several months. It is shown that, in essence, we are talking about strategies for reflexive control, swarm effects of network-centric tools for conducting a "hybrid war" and "controlled chaos" through targeted "acupuncture" effects on "pain" points of the Russian Federation, both worked out in the collapse of the USSR and a number of other states ("Vulnerability points"), when regular and synchronized impacts in the vicinity of the bifurcation point (the transition of a complex macroeconomic system to a new quality of stability or instability / destabilization) should guarantee Anno disrupt macroeconomic and domestic political stability of the Russian state, ie, to achieve results without the direct use of military force, while demonstrating the smashing "NATO power trident", deploying new military contingents and offensive weapons systems in neighboring countries, essentially bringing NATO closer to Moscow with a "pistol shot" with the cocked trigger.*

New threats to the security of Russia associated with the possible implementation of these proposals have been identified. To neutralize them, it was proposed to conduct an objective proactive analysis to identify the threat of socio-political destabilization of Russia at its early stage and to develop timely measures to counter this threat. It is shown that the analysis methods should make it possible to implement a system of continuous monitoring of the degree of this threat in the countries most important for Russia and a decision support system in the field of ensuring socio-political stability of society.

This work was supported by the Russian Federal Property Fund (project 18-011-00567).

Ключевые слова. *Угроза безопасности, корпорация РЭНД, «гибридная война», «управляемый хаос», «точка уязвимости», рефлексивное управление, когнитивная безопасность, стратегия преэмптивной войны.*

Key words. *Security threat, RAND corporation, «hybrid warfare», «controlled chaos», «vulnerability point», reflective management, cognitive security, strategy of a pre-emptive war.*

1. Исходный дискурсивный анализ

Так называемая новая стратегия сдерживания/изматывания, а по сути, развала России посредством ее последовательного и «неминуемого» перенапряжения и изнурения, выраженная в последовавших за последние несколько месяцев друг за другом трёх докладах, рожденных в недрах «мозгового треста» RAND Corporation: «Russia Is a Rogue, Not a Peer; China Is a Peer, Not a Rogue. Different Challenges, Different Responses» («Россия — агрессивна, но не игрок высшей лиги, Китай — игрок высшей лиги, но не агрессивен»), «Overextending and Unbalancing Russia. Assessing the Impact of Cost-Imposing Options» («Слишком большая и несбалансированная Россия). Оценка влияния затратных вариантов») и «Extending Russia. Competing from Advantageous Ground» («Истощение России через расширение ее вовлеченности: противоборство на лучших условиях») на поверку оказывает-

Григорьев Виталий Робертович *– кандидат технических наук, доцент, заместитель директора института, МИРЭА;*
Ковалев Виктор Иванович *– кандидат технических наук, заместитель руководителя секции, АВН, тел. (495)543-36-76.*

Grigoryev Vitaliy *– candidate of technical sciences, associate professor, deputy director of the institute, MIREA;*
Kovalev Viktor *– candidate of technical sciences, deputy head of section, AVN, tel. (495) 543-36-76.*

ся определенной «реинкарнацией» отработанных ранее действий мировой элиты, позволивших развалить Советский Союз. По сути, речь идёт об отработанных и по развалу СССР, и ряду других государств стратегий рефлексивного управления, роевого воздействия сетецентрических инструментов ведения «гибридной войны» и «управляемого хаоса» путем точечного «акупунктурного» воздействия на «болевые» точки РФ («точки уязвимости»), когда регулярные и синхронизированные воздействия в окрестности точки бифуркации (перехода сложной макроэкономической системы в новое качество устойчивости или неустойчивости/дестабилизации) должны позволить гарантированно разрушить макроэкономическую и внутриполитическую устойчивость российского государства, т.е. добиться результата без непосредственного применения военной силы, при этом демонстрируя разящий «силовой трезубец НАТО», размещая в соседних с РФ государствах новые воинские контингенты и системы наступательного вооружения, по сути, приближая НАТО к Москве на расстояние «пистолетного выстрела» при взведенном курке.

Безусловно, что появление этих докладов не случайно, а являются следствием реагирования военно-политической и финансовой элиты США на самостоятельные действия России на протяжении пребывания у власти Президента РФ В.В.Путина, позволившие ей вернуться в строй главных мировых геополитических игроков, а именно:

1) возврат Крыма, возрождение и привязка его экономической инфраструктуры к России, превращение его в непотопляемый авианосец, принципиально изменивший соотношение военно-политических сил в черноморско-средиземноморском регионе, а следовательно, появление у России новых военно-политических возможностей по воздействию на все военно-политические и макроэкономические процессы на Ближнем Востоке и Северной Африке, Балканах, Кавказе и Малой Азии;

2) коренное изменение, а по сути, срыв сценария по уничтожению режима Асада и развала суверенной Сирии, что привело к срыву геополитических расчетов по перекрытию России экспортных возможностей по удержанию Европы на «игле» зависимости от дешевого российского газа; разрушение замыслов продвижения в Европу напрямую по трубопроводам дешевой катарской нефти;

3) создание и успешное на начальной стадии продвижение новых международных экономических союзов в рамках ШОС, ЕврАзЭС, БРИКС;

4) активизация центростремительных процессов на постсоветском пространстве в сторону России как объединяющего начала (ОДКБ, экономический союз стран СНГ, поступательное развитие Союзного государства Россия-Беларусь);

5) продвижение российских экономических и военно-политических интересов вопреки многовековой доктрине Монро в самое уязвимое подбрюшье США, а именно появление в Южной Америке, помимо Кубы, лояльных к России правящих режимов (Венесуэла (Чавес-Мадуро), Никарагуа, Боливия, Бразилия, Аргентина;

6) успешная поступательная политика в Прикаспийском регионе, основанная на сотрудничестве с Ираном, (в том числе достигнутая и утвержденная на уровне ООН резолюция по атомной энергетике), Азербайджаном, Казахстаном и Турцией, превращение Каспия практически во внутреннее море с полным доминированием российских ВМС;

7) рост цен на углеводороды в 2000–е годы, позволивший России вновь подняться с колен в экономическом плане, стабилизировать общественно-экономические отношения внутри РФ, увеличить расходы на национальную оборону (возрождение предприятий ВПК, замена устаревших систем вооружений, рост денежного довольствия военнослужащих, повышение их социального статуса и др.) и вернуть большую часть государственного долга внешним кредиторам;

8) высокий рейтинг доверия национальному лидеру В.В. Путину, а следовательно, проводимому им внутри- и внешнеполитическому курсу;

9) относительная устойчивость к международным экономическим санкциям, не приведшим к массовому протесту населения вследствие ухудшающегося экономического положения;

10) неудавшиеся сценарии ненасильственного свержения действующей власти (Болотная площадь, протестные митинги (Навальный и К°.);

11) препятствование влиянию НПО на территории РФ, финансируемых из-за рубежа, а вследствие этого резкое сокращение возможностей раскачивания «российской лодки» изнутри;

12) возросший и показавший эффективность информационный потенциал влияния на западную аудиторию (Russia Today, Sputnik);

13) продвижение российского газа в Европу в обход Украины и Польши (строительство стратегических газопроводов Северный и Южный поток);

14) сближение с геоэкономическим конкурентом США Китаем во всех областях взаимодействия, в том числе в военно-технической;

15) рост и расширение географии продаж российского оружия и систем вооружения по результатам успешно проводимой Россией в Сирии военно-воздушной антитеррористической операции с мировым злом в лице ИГИЛ, а соответственно рост конкуренции на этом рынке;

16) частичное возрождение патриотических традиций (движение «Бессмертный полк»), вопреки насаждаемым в течение последних десятилетий западным ценностям, осуждение на официальном уровне гендерной революции и её последствий (однополые браки, публичные акции и марши);

17) крупные и знаковые достижения в росте международного авторитета России при проведении ею в качестве «мягкой силы» крупных мировых форумов (зимняя Олимпиада в Сочи, ЧМ по футболу в 2018 г.), позволившие во многом разрушить мифологизацию России как империи зла, на что были затрачены огромные финансовые средства, которые перестали окупаться;

18) инициатива перехода на бездолларовые расчеты при покупке российских нефти и газа во взаимо-

расчетах с Китаем и др. странами;

19) уменьшение вклада России в американские гособлигации.

Очевидно, что самостоятельная, по крайней мере, в политической сфере политика России и постепенный её выход из экономической пропасти 90х годов XX столетия, когда Запад посчитал уже невозможным её возрождение, складывающаяся благоприятной обстановка на рынке углеводородов, положительный имидж России после ее эффективного вмешательства в сирийский вопрос и ее победного результата в борьбе действительно с мировым злом в лице ИГИЛ, породили рост международного влияния России и возвращение ее на позицию сверхдержавы, от мнения, а тем более от действий которой зависит развитие мировой стабильности во всех уголках планеты, и по сути установление многополярного мира в новой формации.

В этой связи, безусловно, интересно одновременное появление, а тем более публичное обнародование сразу нескольких докладов с указанием набора действий относительно России, дабы сдержать ее развитие, а самое главное не позволить России сплотить вокруг себя бывшие страны СНГ, и тем самым возродить в новом виде бывший СССР с его могучими вооруженными силами.

Однако возникает ощущение, что такая демонстративная публичность и синхронизированность появления сразу трех докладов, является ничем иным, как отработанным на протяжении многих лет способом рефлексивного управления ситуацией, которая должна побудить Россию на «реактивные» действия именно по тем направлениям, которые «глубоко проанализированы» в этих докладах.

2. Новые угрозы когнитивной безопасности России

Исходя из анализа доклада корпорации РЭНД «Истощая Россию. Борьба с выгодных позиций» можно сделать вывод о том, что в настоящее время Администрация США рассматривает возможности перехода к новой фазе конфликтного противостояния США – Россия от активной «демонстрационной» фазы к собственно военной фазе нового типа («гибридная война»). При этом, как это прямо следует из определения концепта «война», данного Лидделом Гартом, выживание противостоящего «актора» конфликта (России) уже не принимается в качестве ограничивающего условия при определении масштаба и вида применяемых технологий направленного воздействия на нее.

Социально-политическая дестабилизация обществ с помощью широкого спектра технологий (от втягивания в гонку вооружений и экономического «истощения» до «управляемого хаоса» и «цветных революций») в настоящее время является широко распространенным и эффективным методом ведения «гибридных» войн. Указанный выше доклад РЭНД Корпорейшн «Истощая Россию. Борьба с выгодных позиций» (2019 г.) свидетельствует, что США перешли от совокупности недружественных акций к системной, планомерной работе по расшатыванию экономики и политической системы России, воздействия на ее уязвимости в различных сферах жизни с целью доведения ее до кризисного состояния с последующим самораспадом страны (как это произошло с СССР) при минимизации затрат со стороны США.

В сфере воздействия на индивидуальное, групповое и массовое сознание российской стороны происходит переход от совокупности информационно психологических операций и кампаний к массированному комплексному многоканальному воздействию с задействованием как собственно технологий информационно – психологического воздействия (ИПВ), так и других "невоенных" способов, в качестве которых рассматривается целый спектр различных мер, основными из которых рассматривается вытеснение России с рынка энергоносителей, а также вовлечение ее в новую гонку вооружений. При этом в качестве одного из способов воздействия рассматривается дальнейшая дипломатическая и экономическая изоляция Российской Федерации. Цель такого комплексного воздействия − достижение *синергестического* эффекта. Для организации эффективного направленного воздействия предлагается поиск «точек уязвимости» России.

В существующих геополитических реалиях в докладе не выделен «универсальный» метод воздействия. Так, повышение уровня конкуренции на рынке энергоносителей и тем более гонка вооружений весьма затратны для экономики США. Складывается мнение, что дальнейшие действия Администрации США будут ситуативными, т.е. определяться ответными действиями Российской Федерации. Более того, часть действий может носить так называемый «фейковый» характер – создание видимости какой-либо ситуации для стимулирования принятия мер реагирования на них российской стороной.

Проведенный анализ информационного поля показал, что после публикации анализируемого доклада США и их союзниками неоднократно осуществлялись информационно-психологическое воздействие в виде якобы имевшей место демонстрации силы.

Пример 1. «Объединенный комитет начальников США 11 июня [2019 г.] то ли по ошибке, то ли вполне осознанно выложил на короткое время в открытый доступ новую доктрину о ядерных операциях Пентагона. Документ был через некоторое время удален с сайта ведомства, но в сеть он утек»[1].

Пример 2. «Места размещения ядерного оружия США оказались случайно раскрыты в докладе комитета Парламентской ассамблеи НАТО, сообщает Washington Post [16 июля 2019 г.]. Копия доклада была опубликована бельгийской газетой De Morgen во вторник. В нем отмечается, что "бомбы хранятся на шести американских и европейских базах — Kleine Brogel в Бельгии, Büchel в Германии, Aviano и Ghedi-Torre в Италии, Volkel в Нидерландах и Инджирлик в Турции"»[2] .

[1]https://alexandr-palkin.livejournal.com/2019/07/02/.

[2]https://forum-msk.org/material/news/15774167.html.

Параллельно в прессе [18 июля 2019 г.] появляются сообщения о возможных потенциальных изменениях на рынке энергоносителей: «к 2022 г. планируется реализовать проект газопровода Baltic Pipe, благодаря которому Польша получит доступ к норвежской газовой сети» .

Не исключено, что осуществляются попытки повлиять или выяснить реакцию Российской Федерации по другим направлениям, обозначенным в докладе РЭНД.

Можно, конечно полагать, что рассматриваемый блок докладов корпорации РЭНД это:

• во первых, всего лишь частное мнение ведущих американских аналитиков;

• во вторых, одна из его главных задач – *рефлексивное управление* российской стороной, в чем американцы усилиями В.Лефевра весьма преуспели (скорее всего с этим можно согласиться).

Однако в обосновании серьезности связанных с докладами вызовов и угроз необходимо отметить следующее.

Во первых, уже 27 июня 2019 г. на сайте организации USAID опубликован доклад «Countering malign Kremlin influence development framework».

Справочно. Агентство США по международному развитию (англ. United States Agency for International Development, USAID) — высший федеральный орган государственного управления Соединённых Штатов Америки в области оказания «помощи» за рубежом. Администратор Агентства и его заместитель назначаются президентом с согласия Сената и действуют в координации с государственным секретарём США.

Данный доклад необходимо отметить в связи с тем, что предлагаемые в докладе меры по сдерживанию Российской Федерации (за исключением военной сферы и предлагаемой гонки вооружений, не попадающих в область интересов USAID), в значительной степени коррелируют с упомянутым выше докладом корпорации РЭНД. В частности, предлагается выявление и пресечение попыток Российской Федерации влиять на выборные процессы в других странах, выявление и пресечение попыток распространения дезинформации в зарубежных средствах массовой информации, вытеснение России с рынка энергоносителей, экономическая изоляция России в целом.

Во вторых, материал указанных докладов прямо соответствует недавно принятым стратегическим документам Армии США. Он можно сказать обосновывает (фундирует) их.

Как было отмечено известными военными аналитиками (Е.С.Лариной и В.С.Овчинским), в начале октября 2014 г. в США была обнародована новая оперативная концепция сухопутных войск США - «Победа в сложном мире 2020-2040 гг.».Главное в концепции то, что впервые на уровне официального документа было обнародовано принципиально новое видение облика войны Соединенными Штатами.

Анализ концепции позволяет сделать вывод о том, что произошло качественное изменение формата проектирования Штатами своего места и роли в мире. Концепция определяет −ем американские стратеги видят предназначение войны и армии в следующие 20 лет XXI века, и как собираются превентивно ликвидировать потенциальные угрозы, важнейшими из которых по-прежнему являются финансовое, энергетическое и идеологическое господства.

Это последний из документов, оформивших так называемую «стратегию преэмптивной войны»: использование войны как средства уничтожения потенциальных геополитических и экономических конкурентов прежде, чем они приобретут достаточную мощь, чтобы блокировать доминирование США в мире.

Разработаны контуры нового варианта упреждающей стратегии и соответствующий ей инструментарий и методы.

Преэмптивная война предполагает уничтожение потенциальной угрозы противника, когда нападение его не неизбежно или даже вовсе им не планируется. При этом интенсивность конфликтов, его участники, поля боя и сферы противоборств являются переменными величинами.

Можно выделить следующие особенности концепции.

1. Постулируется, что между войной и миром нет больше четкой грани. Поэтому новая преэмптивная стратегия будет реализовываться не только в ходе традиционных военных конфликтов, а рамках жестких противоборств. Фактически речь идет о том, что появляется новое состояние - "миро-война" или "войномир", уже достаточное для осуществления упреждающих действий по устранению потенциальных, возможных в будущем угроз.

2. В теоретическом и в практическом смысле вся военная доктрина США направлена на задачу подавления воли противника, его подчинения, превращения в средство достижения собственных целей.

3. Исходя из предпосылки, что среда, враги, местонахождения и коалиции, участвующие в будущих конфликтах, неизвестны, армия США готовит стратегию войны против всех государств и народов.

В таких условиях стратегическая цель армии – «применение возможностей или использования тактики таким образом, что сделать невозможным эффективную реакцию противника».

4. Многовариантность превентивных реакций США, ответов на «асимметричное оружие» с использованием всего политического и экономического потенциала, чтобы «воздействовать на врагов, которые будут противостоять США с помощью «общественного восприятия [событий], политических диверсий, преступности и пропаганды».

5. Значительно расширяются сферы противоборств, в которых совершаются упреждающие военные действия.

Впервые официально признаны сферами войн:

• противоборства в сфере дипломатии;

• внутриполитические гражданские конфликты;

[3]https://www.pravda.ru/news/world/1389354-pipeline.

[4]https://www.usaid.gov/documents/1863/countering-malign-kremlin-influence-development-framework.

• информационные войны;
• финансово-экономические войны;
• жёсткое технологическое противоборство.

6. Важным элементом новой концепции являются «поведенческие войны» (целенаправленные воздействия на поведение больших групп населения и элитных структур стран − потенциальных источников вероятных угроз). Важно понять, что для США победа в каждом эпизоде войны или даже в войне – не всегда важны. Главное разрушить возможности своего врага – России к сопротивлению, ведению войны, при постоянной возможности всегда и везде усилить нажим или нанести удар.

Новым фактором войны является современное и предельно циничное стратегическое целеполагание США, основанное на замысле достижения победы в войне путем «цивилизационного стирания противника».

Исходя их данных обстоятельств необходимо со всей серьезностью отнестись к рассматриваемым докладам.

Как уже было отмечено ранее, часть мероприятий с противостоящей стороны уже реализуется в виде информационно-психологического воздействия с целью принятия решений, политически выгодных руководству США и их союзников.

Отсутствие юридически обязывающих норм международного права в сфере использования информационно коммуникационных технологий (ИКТ) в контексте глобальной безопасности привели к тому, что НАТО разработал в 2013 г. правовые рамки для легализации актов агрессии в инфосфере – «Руководство по международного праву, применимому ведению военных действий в киберпространстве» («Tallinn Manual»). В феврале 2017 г. вышло второе его издание, которое более комплексно легализует милитаризацию киберпространства[1].

В «кибервойнах» особую сложность представляет собой достоверное выяснение как мотивов компьютерных атак, так и источника угрозы (госструктуры, сообщества хакеров, отдельные лица), что имеет принципиальное значение для возникновения права на самооборону согласно ст. 51 Устава ООН. Создание в Риге центра НАТО по стратегическим коммуникациям (информационному противоборству), учреждение НАТО совместно с ЕС в Хельсинки Центра противодействия гибридным угрозам (против России), а также регулярное проведение НАТО массированных киберучений резко повышают актуальность разработки мер противодействия, включающих защиту от информационных угроз, организацию активных форм противодействия и нейтрализацию последствий.

В целом указанные, а также иные не рассмотренные в данном документе факты позволяют сделать вывод о появлении новой угрозы, связанной с организацией массированного комплексного многоканального направленного воздействия, нацеленного на выявленные «окна уязвимости» России с задействованием как собственно технологий информационно – психологического воздействия (ИПВ), так и других «невоенных» способов. Противником ведется информационная война нового типа, включающая элементы гибридного воздействия.

Нарастающие масштабы и сложность гибридных войн требует организации мониторинга новых вызовов, опасностей и угроз, связанных с задействованием технологий информационных войн нового типа, создания современных адекватных механизмов защиты от информационных угроз, организации активных форм противодействия и нейтрализации последствий.

Выводы

Необходим объективный упреждающий анализ, позволяющий выявить угрозу социально-политической дестабилизации России на ранней ее стадии и выработать своевременные меры по парированию этой угрозы. При этом методики анализа должны позволять реализовать систему постоянно действующего мониторинга степени данной угрозы в наиболее важных для России странах и систему поддержки принятия решений в области обеспечения социально-политической устойчивости общества.

В связи с этим для решения данной проблемы должен применяться междисциплинарный подход, подразумевающий рассмотрение проблем в широком историческом, экономическом, культурном, цивилизационном аспектах на основе совместной работы политологов, социологов, экономистов, демографов, историков, математиков, психологов и др.

[1]https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf (дата обращения 19.03.2017).

Материал поступил в редакцию 20.09.2019 г.

УДК 342.3, 321.011

© Ромашкина Н.П.
© Romashkina N.

ИНФОРМАЦИОННЫЙ СУВЕРЕНИТЕТ В СОВРЕМЕННУЮ ЭПОХУ СТРАТЕГИЧЕСКОГО ПРОТИВОБОРСТВА

INFORMATION SOVEREIGNTY IN THE MODERN ERA OF STRATEGIC WARFARE

Аннотация. *В статье представлен научный подход к определению понятия «информационный суверенитет», выявлению и постановке проблемы информационного суверенитета в условиях наступившей эры стратегического противоборства с применением информационно-коммуникационных технологий (ИКТ), а также значимости обретения и укрепления такого суверенитета для России. На основе анализа современных угроз в информационной сфере обоснован вопрос о необходимости создания Стратегии информационной безопасности Российской Федерации.*

Abstract. *The article presents a scientific approach to the definition of "information sovereignty," the identification and formulation of the information sovereignty problem in the conditions of the new age of strategic warfare with information and communication technologies (ICT), as well as the importance of that sovereignty for Russia. Based on the analysis of modern informational threats, the question of the need to create an Information Security Strategy of the Russian Federation is substantiated.*

Ключевые слова. *Информационный суверенитет, стратегическое противоборство, стратегия информационной безопасности, информационное пространство, информационная безопасность, законодательное обеспечение, технологии (ИКТ).*

Key words. *Information sovereignty, strategic confrontation, information security strategy, information space, information security, legislative support, technologies (ICT).*

Об информационном суверенитете

Обретение и укрепление информационного суверенитета является в цифровую эпоху одной из важнейших функций государства. В настоящее время нет единого общепринятого понимания понятия «информационный суверенитет». Но, исходя из определения термина «суверенитет» как независимости государства во внешних делах и верховенства государственной власти во внутренних делах, логично рассматривать информационный суверенитет как способность технологически и законодательно обеспечивать и защищать независимость государства и конституционные права граждан в информационном пространстве от внешних угроз (независимость государства во внешних делах), контролируя при этом происходящее в этом пространстве (верховенство государственной власти во внутренних делах) (см. рис.1). Отсутствие такого полномасштабного государственного контроля приводит потенциального противника к опасному осознанию возможности безнаказанной агрессии с применением информационно-коммуникационных технологий (ИКТ) вплоть до уничтожения государства как института. Примеры подобных ИКТ-нападений мы наблюдаем в нарастающих масштабах с конца 90-х годов XX столетия до настоящего времени.

Сегодня полнотой информационного суверенитета не обладает ни одно государство, но его уровень в разных странах различный. Для России необходимость совершенствования законодательного и технологического обеспечения независимости государства в информационном пространстве является сегодня стратегической целью. Одной из важнейших задач для ее достижения является создание законодательной базы (см. рис. 1).

Что является необходимым для законодательного обеспечения информационного суверенитета?

1. Сбор и анализ информации о состоянии и проблемах законодательства РФ, регулирующего вопросы безопасности в сфере ИКТ, развития и использования цифровых технологий.

2. Мониторинг законодательства РФ и иностранных государств, регулирующих вопросы информационной безопасности при использовании цифровых технологий. Эта работа должна вестись экспертами по инициативе и по запросу парламента на постоянной основе. И тогда это приведет к постоянному совершенствованию законодательства, и, как следствие, к постоянному совершенствованию государственной политики в этой сфере.

3. Совершенствование законодательства РФ, регулирующего вопросы развития и использования цифровых технологий, информационной и технологической безопасности.

Научная постановка проблемы информационного суверенитета

Признаки наличия проблемы

1. Несогласованность между современными ИКТ (большие данные, облачные технологии, суперкомпьютеры, искусственный интеллект и т.д.) и законо-

Ромашкина Наталия Петровна *– кандидат политических наук, профессор, руководитель подразделения проблем информационной безопасности, ЦМБ ИМЭМО РАН, тел.+7(926)247-46-25.*

Romashkina Natalia *– Ph.D. (political science), professor, head of the information security issues unit, Center for International Security, IMEMO RAN, tel. + 7 (926) 247-46-25.*

Рис 1. Понятие «информационный суверенитет»

дательством РФ, регулирующим вопросы безопасности в сфере ИКТ, развития и использования цифровых технологий. Например, несмотря на лавинообразный рост возможностей для сбора в Интернете личных данных граждан (персональные данные являются их частью) и использования их массивов (так называемых «больших данных»), до сих пор эта сфера не упорядочена и не введена в правовое поле. При этом такие информационные массивы могут использоваться во вредоносных целях и перепродаваться, например, для слежки, шантажа, пропаганды и т.д. Кроме того, эти данные накапливаются и могут быть использованы против человека спустя много лет. Таким образом, законодательное регулирование таких процессов является частью информационной безопасности государства.

2. Неоднозначность положений некоторых законов, которые по-разному трактуются государственными регуляторами и операторами и требуют конкретизации, уточнений и разъяснений. Кроме того, существует проблема терминологии. В ООН по инициативе России используется компромиссный термин «информационно-коммуникационные технологии» (ИКТ). В официальных документах РФ также отсутствует термин «кибер», «кибернетический», «кибербезопасность» и т.д. Но при этом в технических регламентах и ГОСТах термин «кибер» активно используется.

3. Сложность и дороговизна системы технической защиты информационных систем персональных данных.

4. Зависимость информационной безопасности РФ от иностранных поставщиков программно-аппаратных компонентов программного обеспечения (ПО) и оборудования. Так, большинство интернет-технологий (браузеры, поисковики, социальные сети, операционные системы и др.) находится вне пределов российского контроля. Это создает дополнительные угрозы безопасности. Поэтому для обеспечения своего суверенитета государству следует иметь полную технологическую цепочку, начиная от процессора и заканчивая конечным ПО.

5. Уязвимость элементов информационной безопасности в финансовом секторе РФ в связи с нехваткой квалифицированных специалистов, программного обеспечения и недостаточной координации с правоохранительными органами. Необходимость использования системы SWIFT для международных расчетов.

6. Несовершенство информационной безопасности в социальной и образовательной сферах.

7. Опережение развития атакующих ИКТ-технологий по сравнению с защитными у лидеров ИКТ-индустрии (в частности, в отношении сведений, содержащих государственную или коммерческую тайну, а также серверов государственных учреждений и других объектов критически важной государственной инфраструктуры), что требует постоянного мониторинга законодательства РФ и иностранных государств, регулирующих вопросы информационной безопасности.

8. Рост рисков ущерба репутации государства в связи с вредоносным использованием ИКТ в политической конкуренции, что может выражаться не только в репутационных, но и в финансовых потерях.

9. Необходимость адаптации законодательства РФ к глобальным угрозам информационной безопасности на международном уровне (в частности, разработка и принятие Стратегии информационной безопасности РФ).

10. Целесообразность гармонизации и унификации законодательств государств - союзников и партнеров РФ в сфере информационной безопасности в условиях формирования глобального информационного пространства и ускоренного роста глобальных угроз информационной безопасности.

11. Необходимость совершенствования законодательства РФ, способствующего созданию международной нормативно-правовой базы по борьбе с ИКТ-угрозами.

Постановка проблемы

Повышение значимости обеспечения информационной безопасности в качестве системообразующего элемента управления, а также совершенствова-

ние правового обеспечения в ИКТ-сфере стало на современном этапе одним их основных стратегических приоритетов государственной политики. В настоящее время законодательство РФ в сфере ИКТ переживает стадию роста и не отвечает всем требованиям, позволяющим обеспечить информационную безопасность в полном объеме.

Таким образом, основной целью на современном этапе является создание механизма, позволяющего согласовать процесс разработки законов с существующими реалиями и прогрессом ИКТ для обеспечения информационного суверенитета и безопасности государства.

Основные задачи для достижения этой цели связаны с качеством государственного управления и уровнем информационной безопасности, которые в целом определяются способностью государства:

1) обеспечить функционирование информационных ресурсов и потоков, необходимое и достаточное для устойчивой жизнедеятельности и развития; противостоять техническим и психологическим угрозам, оградить систему и пользователей от негативного ИКТ-воздействия;

2) защитить в полном объеме государственную и коммерческую тайну от незаконных посягательств;

3) поддерживать эффективность работы, возможность «саморазвития» и адекватные реакции системы на возрастающие вызовы;

4) обеспечить устойчивость и безопасность государства от ИКТ-угроз в военно-политической сфере.

Первостепенными задачами экспертного сообщества при этом являются:

1) подготовка предложений и рекомендаций, включающих в себя результаты традиционных методов формально-юридических исследований для выявления внутрисистемных противоречий и социально-правовых проблем в сфере ИКТ, а также методов политологических исследований для выявления межсистемных противоречий и политических проблем;

2) разработка методологии выявления правовых проблем в ИКТ-сфере, а также общих социально-политических условий подготовки и принятия законодательных актов для постоянного совершенствования законодательства в сфере информационных технологий.

Таким образом, результатом деятельности экспертов из разных областей должно стать создание постоянно действующего механизма, который позволит согласовать процесс разработки законов с существующими реалиями и прогрессом ИКТ для обеспечения информационного суверенитета и безопасности государства. В обозримой перспективе этот механизм целесообразно настроить на применение комплексного подхода:

1) внесение изменений в существующее законодательство, исходя из анализа практики применения и новых условий, связанных с ускоренным развитием ИКТ;

2) параллельная работа по подготовке Стратегии информационной безопасности РФ;

3) подготовка новых нормативно-правовых актов после выхода Стратегии информационной безопасности РФ.

Новая эра стратегического противоборства

В сентябре 2018 г. в США была утверждена новая Национальная киберстратегия (National Cyber Strategy of the United States of America)[1]. Предыдущая киберстратегия была принята в США 15 лет назад. Анализ структуры документа, представленной на рис 2, позволяет делать выводы о качестве его подготовки.

Не возвращаясь к детальному анализу новой Киберстратегии США, целесообразно напомнить лишь некоторые цитаты.

1. «В настоящей стратегии излагаются методы, с помощью которых моя администрация будет:

• обеспечивать безопасность Америки путем защиты сетей, систем, программных функций и данных;

• обеспечивать процветание Америки путем построения безопасной, успешной цифровой экономики и стимулирования развития инноваций на национальном уровне;

• обеспечивать мир и безопасность путем увеличения возможностей США совместно с их союзниками и партнерами по сдерживанию, а при необходимости и по наказанию лиц и государств, использующих цифровые инструменты в злонамеренных целях;

• расширять американское влияние за рубежом с целью более широкого внедрения основных принципов открытого, функционально совместимого, надежного и безопасного интернета».

2. ««Россия, Китай, Иран и Северная Корея используют киберпространство в качестве площадки, где они могут бросить вызов Соединенным Штатам, нашим союзникам и партнерам… Россия, Иран и Северная Корея провели ряд хакерских атак, которые нанесли ощутимый ущерб американским и транснациональным компаниям, нашим союзникам и партнерам и не понесли соответственного наказания, что могло бы стать сдерживающим фактором от осуществления подобных хакерских атак в будущем. Китай использует киберпространство для осуществления экономического шпионажа и кражи объектов интеллектуальной собственности, стоимость которой измеряется триллионами долларов».

3. «Нынешняя администрация уже приняла ряд мер по активному устранению этих угроз и адаптации к новым реалиям. Мы наложили на опасных внешних злоумышленников соответствующие санкции. Мы поименно назвали наших противников, осуществлявших подрывную деятельность, и опубликовали информацию о совершенных действиях, а также используемых ими инструментах и методах. Мы обязали государственные органы и ведомства заменить программное обеспечение, имеющее критические уязвимости для обеспечения безопасности».

4. «Соединенные Штаты намерены сотрудничать с государствами-единомышленниками по вопросам координации и оказания поддержки применения мер реагирования друг друга в отношении серьезных злоумышленных инцидентов в киберпространстве, в том числе посредством обмена разведывательными дан-

Структура национальной киберстратегии США-2018

ВВЕДЕНИЕ
Анализ текущей ситуации
Стратегия развития

СТОЛП I: Защита американского народа, Америки и американского образа жизни

Безопасность федеральных сетей и информации
Дальнейшая централизация управления и контроля в сфере федеральной гражданской кибербезопасности
Согласование деятельности в области управления рисками и информационных технологий
Совершенствование управления рисками в федеральной системе поставок
Укрепление кибербезопасности федеральной контрактной системы
Обеспечение лидирующей роли правительства в области передовой и инновационной практики
Безопасность критически важной инфраструктуры
Уточнение ролей и обязанностей
Приоритетность действий в соответствии с выявленными национальными рисками
Использование поставщиков ИКТ в качестве средств обеспечения кибербезопасности
Защита нашей демократии
Стимулирование инвестиций в кибербезопасность
Приоритетность инвестиций в национальные исследования и разработки
Совершенствование транспортной и морской кибербезопасности
Совершенствование Космической Кибербезопасности
Борьба с киберпреступностью и совершенствование отчетности об инцидентах
Совершенствование отчетности об инцидентах и реагировании на них
Модернизация законов об электронном наблюдении и компьютерной преступности
Снижение угроз со стороны транснациональных преступных организаций в киберпространстве
Совершенствование системы задержания преступников заграницей
Усиление правоохранительного потенциала стран-партнеров для борьбы с киберпреступностью

СТОЛП II: Обеспечение процветания Америки

Содействие динамичной и устойчивой цифровой экономики
Стимулирование развития рынка адаптивных и безопасных технологий
Приоритеты инновационной деятельности
Инвестиции в инфраструктуру следующего поколения
Содействие свободному трансграничному потоку данных
Сохранение лидерства США в передовых технологиях
Продвижение кибербезопасности с полным жизненным циклом
Содействие развитию и защита изобретений в США
Совершенствование механизмов анализа иностранной инвестиционной деятельности в США
Поддержание сильной и сбалансированной системы защиты интеллектуальной собственности
Защита конфиденциальности и целостности американских идей
Развитие исключительных человеческих ресурсов, обеспечивающих кибербезопасность
Создание и поддержание конвейера талантов
Расширение возможностей переквалификации и образования для американских рабочих
Повышение уровня федеральных специалистов по кибербезопасности
Использование исполнительной власти для выявления и поощрения талантов

Рис 2. Структура национальной киберстратегии США-2018

ными, подкрепленными источниками, публичными заявлениями о поддержке мер реагирования, а также совместным применением мер реагирования против злоумышленников».

5. «Наши конкуренты реализуют программы подготовки трудовых ресурсов, которые могут нанести вред конкурентоспособности Соединенных Штатов в сфере кибербезопасности в долгосрочной перспективе. Правительство Соединенных Штатов продолжит финансировать и расширять программы, которые создают качественный национальный кадровый резерв как в начальной школе, так и в рамках высших учебных заведений. Нынешняя администрация будет внедрять предложенные Президентом иммиграционные реформы, основанные на заслугах кандидатов, с целью создания в Соединенных Штатах наиболее конкурентоспособного технологического сектора».

Кроме Национальной киберстратегии в США, действует Киберстратегия Министерства обороны США [2], а также Стратегия Объединенного киберкомандования Вооруженных сил США (функциональная структура, объединяющая более 6000 специалистов из разных военных ведомств и командований) под названием «Завоевание и удержание господства в киберпространстве». Важное значение в этом контексте имеет также решение НАТО «задействовать статью 5 Устава Альянса о коллективной самообороне при кибернападениях при том, что сама кибероборона возможна не только в рамках крупной операции Альянса» [3].

Следовательно, в США существует очень четкая комплексная стратегическая программа обеспечения и поддержания информационного превосходства путем повышения своих возможностей и всестороннего снижения способностей других акторов.

Таким образом, речь сегодня идет уже не о предпосылках возникновения новой сферы соперничества в информационном пространстве, а о том, что новая эра стратегического противоборства – ИКТ-противоборства – с указанием лидера, противников (не потенциальных, а существующих, по мнению лидера), детального пошагового системного плана действий в ходе борьбы, а также конкретных мер противодействия и «наказания» противников уже наступила. А Россия названа первой в списке врагов лидера информационного пространства, владеющего продуманной стратегией дальнейших действий и побед…

Почему России нужна стратегия информационной безопасности?

Стратегические документы, в правовой форме определяющие направления и перспективы развития государства (а ИКТ являются одним из важнейших характеристик развития в настоящее время) имеют важнейшее значение на современном этапе. Именно они создают правовой фундамент инновационного развития, определяя основы государственной политики.

Важнейшими характеристиками стратегии как правового документа, в отличие от всех других видов нормативно-правовых актов, в частности, являются следующие:

1) целевой подход к разработке, основанный на определении важнейшей цели и задач на пути ее достижения, приоритетность которых определяет содержание и сущностные результаты действий по развитию соответствующей сферы;

2) системный подход к реализации, предусматривающий решение указанных задач и, соответственно, максимальный охват всех основных направлений, которые должны быть задействованы в реализации стратегических установок государственной политики в соответствующей области;

3) комплекс конкретных согласованных и взаимос-

вязанных мероприятий, средств и ресурсов, обеспечивающих достижение результатов, предусмотренных указанными задачами в рамках каждого из приоритетных направлений;

4) действия по единому поэтапному плану с четко обозначенными целевыми индикаторами и показателями на каждом из этапов, а также разработанной системой финансирования основных мероприятий;

5) мониторинг за ходом реализации стратегии и применение системы мер юридического контроля за достижением конечных и промежуточных результатов.

Таким образом, стратегия разрабатывается в рамках определения цели и постановки задач, прогнозирования, планирования и программирования на федеральном уровне, на уровне субъектов Российской Федерации и на уровне муниципальных образований. Очевидно, что Стратегия как система формально-определенных положений, закрепляющих стратегическую цель, задачи и направления деятельности органов государственной власти по ее достижению, средства и ресурсы, которые могут быть на это затрачены, существенно отличается от Доктрины (в России действует Доктрина информационной безопасности [4]), которая по сути представляет собой философскую, политическую либо правовую теорию, концепцию, учение, систему воззрений, руководящий теоретический или политический принцип.

В рамках цели обретения и сохранения информационного суверенитета Стратегия информационной безопасности России должна стать правовым фундаментом развития информационной сферы в стране, обеспечивающим организационные, законодательные и экономические условия и гарантии безопасного эволюционного процесса. Документ призван формулировать цель и задачи развития, а также защиты от угроз и рисков в информационном пространстве. Стратегия должна описывать комплексный системный подход к реализации указанных цели и задач, согласованные и взаимосвязанные действия и мероприятия, которые базировались бы на целевых индикаторах и показателях на каждом этапе реализации. Важной частью стратегии является также четко прописанная система мониторинга и мер юридического контроля за достижением конечных и промежуточных результатов. Такой документ может сыграть важную роль в создании концепции сдерживания агрессивных действий в условиях новой эры стратегического ИКТ-противоборства.

Литература

1. National Cyber Strategy of the United States of America, SEPTEMBER 2018. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
2. DEPARTMENT OF DEFENSE CYBER STRATEGY 2018. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_.
3. НАТО готова к коллективной обороне при кибератаках, но не во всех случаях. URL: http://ria.ru/world/20160614/1447513284.html#ixzz4Be5c0CYs.
4. Доктрина информационной безопасности Российской Федерации. URL: http://www.scrf.gov.ru/documents/5.html.

Материал поступил в редакцию 18.09.2019 г.

УДК 32.019.5

© Маковский В.А.

© Makovskiy V.

«ПЯТАЯ ВЛАСТЬ» КАК ОСНОВНАЯ УГРОЗА ФУНКЦИОНИРОВАНИЯ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ ПОЛИТИКИ В РОССИИ

«THE FIFTH ESTATE» AS A CRITICAL THREAT OF STATE INFORMATION POLITIC'S FUNCTIONING

Аннотация. *Статья посвящена новому социальному явлению - «пятой власти»: подробно рассмотрены причины возникновения, степень влияния на функционирование государственной информационной политики, роль в формировании общественного мнения социально-активного населения страны; предложены варианты нивелирования внутренних и внешних информационных атак.*

Abstract. *The article is devoted to the new social phenomenon «the Fifth Estate»: causes of occurrence, degree of impact on state information politic's functioning, the role in the forming community-minded people's public opinion; the Author submits some proposal to levelling in- and outside information attacks.*

Ключевые слова. *Пятая власть, государственная информационная политика, общественное мнение, формирование общественного мнения, социальная сеть, информационная атака, информационная война, СМИ.*

Key words. *The Fifth Estate, state information politic, public opinion, social media, information attacks, information wars, mass media.*

С появлением и стремительным развитием новых электронных медиа очевиден тот факт, что государственная информационная политика (ГИП) является важной составной частью внешней и внутренней политики государства. С точки зрения внешней политики: ГИП − это система мер по обеспечению информационной безопасности государства и по созданию положительного имиджа страны на мировой арене. С точки зрения внутренней политики: ГИП − это, с одной стороны, политика государства по отношению к стране, народу, обществу с использованием СМИ; с другой стороны,− политика государства по отношению к самим СМИ.

Таким образом, ГИП представляет собой сложную многоступенчатую систему мер по достижению большого спектра целей и задач как внутри государства, так и за его пределами. На первый взгляд система представляется вполне рабочей. Существует ряд документов и законодательных актов, которые призваны контролировать и регулировать ГИП. Доктрина информационной безопасности содержит множество мер по защите государства и общества от внешнего информационного воздействия, закон о СМИ регулирует работу представителей средств массовой информации, Конституция Российской Федерации определяет права граждан страны на доступность информации. Несмотря на количество законов и документов, в настоящее время в полной мере законодательно не урегулированы взаимоотношения государства, средств массовой информации (СМИ) и гражданского общества. Принятый в 1991 г. закон Российской Федерации «О средствах массовой информации» (представляет собой обобщенные правила, на которых базируется работа СМИ) не отвечает требованиям сегодняшнего дня. С момента издания закон претерпел 22 редакции (последняя датирована 18.04.2018г.), в которых наибольшее количество правок связано с изданиями в сети Интернет. Либеральные достоинства закона о СМИ: свобода слова и доступность информации обернулись своего рода угрозой безопасности с появлением новых электронных медиа, поскольку ответственность за публикацию журналистом недостоверной (непроверенной) информации, способной разрушать политическую систему, фактически отсутствует. Реакцией со стороны государства является Доктрина информационной безопасности (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646), которая служит основной для формирования государственной политики в области обеспечения информационной безопасности Российской Федерации; подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации; разработки целевых программ обеспечения информационной безопасности Российской Федерации, работает фрагментарно и бессистемно, несмотря на относительно недавние изменения в документе.

Первоначально Доктрина информационной безопасности РФ была принята 9 сентября 2000г. В 2016г. была изменена, поскольку утратила свою силу и более не отвечала своей основной функции – обеспечение безопасности, без которой не может существовать политическая стабильность государства.

Основные поправки в новом документы касаются «информационно-психологического воздействия» (ИПВ) на индивидуальное и общественное сознание граждан РФ со стороны иностранных спецслужб,

Маковский Василий Александрович *– слушатель, РАНХ и ГС, e-mail:makovskiy2010@mail.ru.*

Makovskiy Vasily *– student, RANH and GS, e-mail: makovskiy2010@mail.ru.*

а также террористических и экстремистских организаций. В версии 2000 г. понятие «экстремистские организации» отсутствовало, а в качестве источников угроз были названы «диверсионно-подрывная деятельность иностранных специальных служб» и «деятельность международных террористических организаций». Также в доктрине 2016 г. впервые отмечается тенденция к увеличению негативных оценок России в зарубежных СМИ. В предыдущей редакции документа говорилось лишь об «опасности зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур». В версии 2000 г. в качестве одной из опасностей в информационной сфере значилось «создание монополий на формирование, получение и распространение информации в РФ». Документ 2016 г. аналогичного положения не содержит. Отсутствие подобного положения связано с расширением способов получения и распространения информации.

В 2018 г. развитие информационных технологий, открытость информации, в том числе распространяемой зарубежными СМИ, наличие социальных сетей и доступа в Интернет требуют новых правок Доктрины.

Доктрина информационной безопасности должна отражать в том числе и регулирование/контроль информации, проникающей в социальные сети и имеющей «вирусный» эффект (быстрое распространение информации в сети, благодаря публикациям на странице пользователя в социальной сети - перепост). При этом с 01 августа 2014 г. была введена ответственность блогеров за размещение информации в Интернете (Федеральный закон от 05.05.2014 №97-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты РФ по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей»), на практике же данного закона недостаточно. Блогером, согласно закону, считается владелец интернет-сайта или страницы интернет-сайта, на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей. Феномен социальных сетей состоит в том, что публикации (фото, видео, текст), имеющие так называемый «вирусный» эффект, распространяются в сети в кратчайшие сроки, даже если были опубликованы человеком с минимальным количеством подписчиков.

Учитывая глобальный трансграничный характер информационных технологий и скорость их развития, был принят ряд других законов, регулирующих деятельность СМИ. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, также претерпел ряд изменений (последняя редакция от 29.06.2018, вступил в силу с 30.06.2018). Редакции вышеперечисленных законов говорят о быстроменяющейся глобальной ситуации в течение короткого промежутка времени и необходимости регулирования на законодательном уровне свободы обмена информацией в целях обеспечения национальной и личной безопасности граждан государства.

Кроме того, развитие и распространение новых информационных технологий, телекоммуникационных средств передачи информации открывают неограниченные возможности доступа широких масс к большому объему новостных и аналитических материалов в режиме реального времени. При этом важен и тот факт, что всемирная сеть Интернет позволяет получать информацию не только от российских, но и от зарубежных СМИ, что неизбежно влечет за собой угрозу информационной безопасности нашей страны, учитывая условия политической нестабильности, кризис реального сектора экономики и шаткую позицию России в мировом информационном пространстве.

Новые электронные медиа ставят под угрозу эффективность и системность ГИП. Это связано с тем, что практически каждый локальный конфликт внутри любого государства буквально за несколько часов может приобрести международное значение. Молниеносное распространение информации и субъективная трактовка тех или иных фактов СМИ отдельных стран напрямую влияет на политическую стабильность внутри любого государства.

Весьма популярным среди российских исследователей в настоящее время является определение СМИ как четвертой власти: СМИ рассматриваются как самостоятельная общественная сила.

На практике же модель «четвертой власти» не работает в современной ситуации не только в России, но и в развитых странах Запада. Очевидно, что СМИ сегодня способны оказывать серьезное политическое влияние, но только в том случае, когда они становится проводником влиятельных политических организаций и структур.

Г. Альтшулл (американский политолог) сформулировал два закона СМИ: 1) содержание сообщений СМИ в большинстве случаев отражает политику тех, кто их финансирует; 2) СМИ не являются независимыми, несмотря на то, что потенциально способны выступать в качестве самостоятельной силы. По факту же во всех системах СМИ являются агентом тех, кто обладает политической и экономической властью.

Существует прямая зависимость СМИ от процессов накопления капитала. Средства массовой информации стали привлекательными инвестиционными объектами, благодаря которым бизнес может оказывать всевозрастающее политическое влияние на общественное мнение и институты власти. Наиболее распространенной формой взаимодействия между СМИ и бизнесом становятся покупка и их последующее финансирование. По сути СМИ уже во многом утратили функцию выражения общественного мнения и отражают прежде всего интересы финансово-промышленных групп. Процесс монополизации и концентрации СМИ развивается во всех странах мира, поэтому информационные монополии контролируют сегодня связи между элитой, обществом и властью.

Демократическое государство обязано осуществлять нормативно-правовое регулирования информационной среды, в противном случае привилегированные финансово- промышленные группы будут решать, какое государственное управление необходи-

мо в информационном обществе. В таком случае система управления будет не демократической, а суперэлитарной, что затруднит достижение основной цели ГИП− построение демократического информационного общества и вхождения России в мировое информационное пространство.

В современных реалиях так называемая четвертая власть утратила свою самостоятельность и трансформировалась в придаток бизнеса и политики. Вместе с тем, сформировалась «пятая власть»: новое демократическое информационное общество (социально-активное население), которое при помощи современных информационно телекоммуникационных технологий выражают и отстаивают свою точку зрения по вопросам, вызывающим резонанс, и влияют на формирование общественного мнения. К современным информационно-телекоммуникационным технологиям относятся социальные сети, мессенджеры (специальные бесплатные сервисы для мгновенного обмена сообщениями), видеохостинги (сайты, на которых можно выложить видеоряд).

К началу 2019 г. аудитория интернет-пользователей в России среди населения 16+ составила 90 миллионов человек (+3 миллиона человек к прошлому году) и достигла отметки 75,4% взрослого населения страны. При этом больше всего растет доля пользователей, которые используют Интернет только на мобильных устройствах. Такие данные опубликовала компания GfK.

Как отмечают исследователи, последние годы аудитория Интернета растет медленно и в основном за счет подключения к Сети пользователей старшего поколения. Среди молодежи и людей среднего возраста проникновение Интернета близко к предельному уровню.

Так, в среднем за день один пользователь проводит в сети 115 минут в десктопе (с экрана монитора стационарного компьютера или ноутбука), пользователи мобильного Интернета проводят онлайн 104 минуты в день (с экрана мобильного устройства - смартфона), что в совокупности дает порядка 3 часов в день на одного пользователя в сети.

Абсолютным лидером по времени, проводимому в сети, среди тематических групп являются социальные сети – 22% всего времени в десктопе и 24% – в мобайле. 52% россиян ежедневно заходят хотя бы в одну из социальных сетей.

Время на видеоресурсах уже сейчас не уступает времени, проводимому в социальных сетях и составляет 22% всего времени в десктопе. В среднем на одного человека приходится 35 просмотров контентных видеороликов в день независимо от их длительности.

Аудитория мессенджеров продолжает активно расти, их используют 62% россиян в возрасте 12-64 лет. 85% мобильных интернет-пользователей хотя бы один раз за месяц заходят в мессенджеры через мобильные устройства.

По сравнению с традиционными СМИ Интернет обладает рядом преимуществ: мультимедиа (объединяет визуальные, звуковые, печатные и видео-аспекты других СМИ); персонализация (возможность донести информацию через призму отдельных предпочтений пользователя); интерактивность (взаимодействие, диалог и обратная связь между миллионами пользователей по всему миру); отсутствие посредников (возможность прямого доступа власти к населению и, наоборот, населения к власти без вмешательства и манипуляций со стороны СМИ); получение информации в режиме реального времени. Данные особенности привлекают социально-активные группы людей и выводят глобальную Сеть на лидирующие позиции в качестве воздействия, достижения целей и продвижения интересов, в том числе и в сфере политической коммуникации.

Не менее важен и тот факт, что новые технологии не только обладают свойством доносить до аудитории сведения о происходящих событиях, как и все остальные СМИ; они способны также создавать коммуникационные сети для внутри- и межгруппового общения и тем самым делегировать функции по передаче информации и формированию общественного мнения самой аудитории, которая активно вовлекается в процесс, поскольку имеет возможность образовывать любые сообщества и группы по интересам. Трансляция идей не от средств массовой информации, а от пользователей воспринимается как достоверная. Именно поэтому возникновение «пятой власти» нельзя игнорировать. Наоборот, стоит рассматривать ее как ключевое звено ГИП, которое требует особого отношения, контроля и регулирования. Именно «пятая власть» уже сейчас представляется двойственной: с одной стороны, она делает политику более доступной для простых граждан, предоставляет политикам новые возможности влияния на аудиторию (что в целом, при грамотной управлении и использовании, может повышать доверие населения к правящему режиму); а с другой стороны, представляет реальную угрозу, поскольку способна за короткий промежуток времени дестабилизировать обстановку внутри страны (провокации, призывы к насилию и тд.) и негативно влиять на имидж России в мировом информационном пространстве.

Важным регулятором отношений между СМИ, бизнесом, «пятой властью» и обществом должна стать государственная информационная политика.

Таким образом, ГИП сегодня − это система взаимоотношений между СМИ, государством, бизнесом, «пятой властью» и обществом, основной целью которой является сохранение политической стабильности внутри страны, мирное разрешение информационных конфликтов и атак со стороны международных провокационных группировок, повышение уровня доверия к власти, создание положительного имиджа страны на мировой арене.

В этой связи важным является и тот факт, что уровень доверия к институтам власти постоянно снижается. Подобные измерения в России (на основе социальных опросов граждан) ежегодно проводит Левада-центр). Снижение доверия россиян к власти зафиксировал также и ВЦИОМ. И если данные отечественных исследований не так критичны (более половины опрошенных доверяют Президенту и правительству), то результаты американской исследовательской компании Edelman, которая также ежегодно публикует рей-

тинг доверия жителей разных стран мира к общественным институтам и институтам власти, настораживают и требуют большого внимания к данной задаче. В списке стран по общему уровню доверия к институтам власти Россия занимает последнее место с индексом доверия 29 из 100. Она оказалась и в числе лидеров по уровню падения доверия за год: еще в начале 2018 г. индекс доверия в стране составлял 36 пунктов. Россияне оказались на последнем месте уровня доверия к общественным организациям: им в стране доверяют лишь 23% опрошенных по сравнению с 74% в Китае, 59% в Канаде и 47% в Великобритании. То же касается и бизнеса: предпринимателям в России верят лишь 34% опрошенных (80% — в Китае, 58% — в Бразилии, 44% — в Испании). Последнее место Россия занимает и по уровню доверия к СМИ. Медиа в России полностью доверяют только 26% (на 9% меньше, чем в прошлом году). Единственный раздел доклада, в котором Россия не заняла последнее место, — доверие к правительству. Властям доверяют 34% россиян — больше, чем в Мексике, Франции, Бразилии и ряде прочих стран. Вместе с тем, уровень доверия к правительству в России упал сильнее всего: за год показатель снизился сразу на 10%.Такое положение вещей, безусловно, требует пристального внимания, поскольку низкий уровень доверия к институтам власти свидетельствует о том, что основная социально-активная часть населения России доверяет все больше информации, которая поступает через социальные сети и мессенджеры, то есть так называемой «пятой власти».

И это вполне логично. В эру столь быстрого развития новых электронных медиа, повсеместного доступа в Интернет, смартфонов с возможностью здесь и сейчас снимать фото и видео, информация с места события в короткий промежуток времени становится доступна каждому, кто интересуется той или иной темой. Нет необходимости ждать официальной информации федеральных СМИ, к которым уровень доверия максимально низкий. Имея доступ в Интернет, можно фактически стать очевидцем событий и трактовать их, опираясь на свой опыт, знания, предпочтения. И если основная масса социально-активного населения страны негативно относится к происходящему (в том числе и к действиям власти), это становится неким эталоном, обрастает новыми, возможно даже несуществующими подробностями, которые формирует общественное мнение. Именно данный факт является прямой угрозой системного функционирования государственной информационной политики, подрывает авторитет власти, дестабилизирует обстановку внутри страны. Уже сейчас речь идет не просто о технических и технологических инновациях в сфере массовой коммуникации, а о «цифровой» революции, которая способна объединять миллионы людей не только внутри страны, но и за ее пределами.

Актуальными остаются вопросы инертности институтов власти в области ГИП (отсутствие оперативной реакции на информационные деструктивные вбросы иностранных СМИ и сторонников оппозиции, непонимание возможных реакций общества на данную информацию) и, как следствие, особую важность представляет отсутствие алгоритма действий в непредвиденных обстоятельствах, связанных с резонансными инфоповодами.

Уже сейчас основной задачей ГИП должно стать создание общей идеологии, политической идеи, которая объединит социально активных граждан страны во благо государства. Идеология понимается как совокупность систематизированных и рационально организованных политических ценностей, в которых оцениваются отношения людей к действительности и выражаются интересы различных социальных групп. Существование людей невозможно вне совокупности ценностей, идей, представлений и чувств, которые в явной или латентной форме направляют наше мышление и поведение. Необходимо проработать стратегию становления и пропаганды сильной России, способной (с помощью неравнодушного населения и новых электронных медиа в том числе) противостоять внутренним и внешним информационным атакам. Подобные действия позволят нивелировать угрозу функционирования государственной информационной политики.

Литература
1. Василенко И.А. Сравнительная политология, 2014.
2.. Назаров М.М. Массовая коммуникация и общество, Москва 2004,
4.. Старостин А.М. Межнациональные отношения в современной России: «точки кризиса» и «точки роста» // Вопросы гармонизации межкультурных, межнациональных и межконфессиональных отношений: Сборник статей Международной научнопрактической конференции Ростов-на-Дону, 4 декабря 2013 г. ,2016.
5.. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», http://base.garant.ru/12148555/, обновл. 18.06.2014.
6.. Закон РФ от 27.12.1991 N 2124-1 (ред. от 06.06.2019) "О средствах массовой информации" (с изм. и доп., вступ. в силу с 01.09.2019).
7.. Доктрина информационной безопасности Российской Федерации утверждена Указом Президента Российской Федерации от 05.12.2016 года № 646 и опубликована 6 декабря 2016 г.
8.. Сайт Исследовательской компании Edelman https://www.edelman.com/sites/g/files/aatuss191/files/2019-02/2019_Edelman_Trust_Barometer_Global_Report.pdf.
9.. Левада центр https://www.levada.ru/2019/04/25/odobrenie-institutov-vlasti-12/.
10.. ВЦИОМ https://wciom.ru/news/ratings/doverie_politikam/.

Материал поступил в редакцию 17.09.2019 г.

УДК 323.28

© Сереброва А.М.

© Serebrova A.

МЕЖДУНАРОДНЫЙ ТЕРРОРИЗМ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

INTERNATIONAL TERRORISM AS A THREAT NATIONAL SECURITY OF RUSSIA

Аннотация. *В статье рассматривается проблема роста террористической угрозы как следствие изменения мирового политического порядка. Автор анализирует понятие терроризма через призму конвенционального подхода. На основании выделения ключевых характеристик современного терроризма представлены приоритетные цели и направления борьбы с этой угрозой.*

Abstract. *The article considers the problem of the growth of the terrorist threat as a consequence of a change in the global political order. The author analyzes the concept of terrorism through the prism of a conventional approach. Based on the identification of the key characteristics of modern terrorism, priority goals and directions for combating this threat are presented.*

Ключевые слова. *Международный терроризм, террористический акт, направления противодействия.*

Key words. *International terrorism, terrorist act, areas of counteraction.*

В 1997 г. в работе «Великая шахматная доска» Збигнев Бжезинский указал, что «в последнем десятилетии XX в. можно отметить тектонические сдвиги в мировых делах» [1]. Действительно, на рубеже веков мировая политическая система претерпела значительные качественные изменения. Распад Ялтинско-Потсдамской системы ознаменовал переход к однополярному мироустройству, который, в свою очередь, просуществовал не слишком долго. Процессы глобализации способствовали постепенному смещению центра принятия решений по международной проблематике. Наряду с этим появляются новые межгосударственные объединения и усиливаются региональные игроки, что позволяет говорить о формирующейся полицентричной системе международных отношений. Она характеризуется ростом количества акторов, их неравновесным и асимметричным взаимодействием. Данные черты придают этой системе турбулентный характер, что проявляется в увеличении конфликтогенности международной среды.

Демонстрацией рассмотренного выше тренда является рост террористической угрозы. Международный терроризм занимает одну из лидирующих позиций среди глобальных вызовов, стоящих перед современным миром, что подтверждает анализ статистики. Согласно данным Global Terrorism Index[6], за последние 12 лет было совершено свыше 61000 терактов, в результате которых погибло более 140000 человек. При этом, как видно из приведенной ниже диаграммы, если в начале второго десятилетия XXI в. террористическими организациями упор был сделан на масштабе проведенных актов с целью получения как можно большего количества жертв, то в последние годы акценты сменились в сторону количества террористических актов, пусть и с меньшим числом жертв. Подобная тенденция во многом вызвана радикализацией сознания населения, официально не являющихся членами организаций.

По сравнению с общемировой динамикой ситуация в Российской Федерации в отношении количества террористических актов более чем положительная. Согласно статистике, приведенной на рис. 2, к 2012 г. данный показатель уменьшился более чем в 10 раз. Наряду с этим также снизилось количество преступлений террористической направленности.

В то же время вызывает опасения третий показатель – число преступлений террористического характера. Если террористический акт представляет собой доведенное до логического конца действие, результатом которого стало большое количество человеческих жертв, а преступление террористической направленности является по сути сорванным террористическим актов, то преступления террористического характера составляют отдельную группу противоправных деяний, объединенных общими криминологическими характеристиками. Примерами могут служить содействие террористической деятельности или призыв к ее совершению, организация незаконного формирования и т.д. Исходя из вышесказанного, можно сделать вывод о хорошей работе спецслужб, предупреждающих совершение террористических актов, с одной стороны, и в то же время увеличении числа радикально настроенных граждан, готовых применять насилие как метод достижения цели. Таким образом, вопрос противостояния террористической угрозе по-прежнему остается актуальным в контексте российских реалий. Вместе с тем, когда речь заходит о терроризме, не до конца ясно, с чем именно борется мировое сообщество, поскольку вплоть до настоящего момента ни на конвенциональ-

Сереброва Анастасия Михайловна *– соискатель кафедры глобалистики факультета глобальных процессов, МГУ имени М.В. Ломоносова, e-mail: aserebro23@yandex.ru.*

Serebrova Anastasia *– applicant for the department of global studies, faculty of global processes, Lomonosov Moscow State University, e-mail: aserebro23@yandex.ru.*

ном уровне, ни в академических кругах не выработано единого подхода к определению данного феномена.

сительно эффективности превентивного подхода к насилию, природы экстремизма, выявление условий и

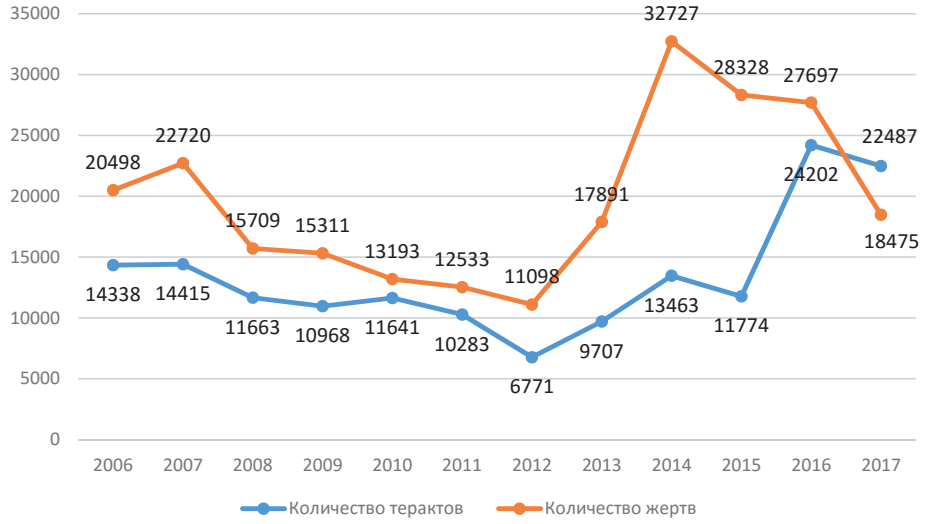


Рис. 1. Количество террористических актов и погибших в результате них в мире за период 2006–2017 гг. (Источник: Global Terrorism Index 2017: Measuring and understanding the impact of terrorism) [6]

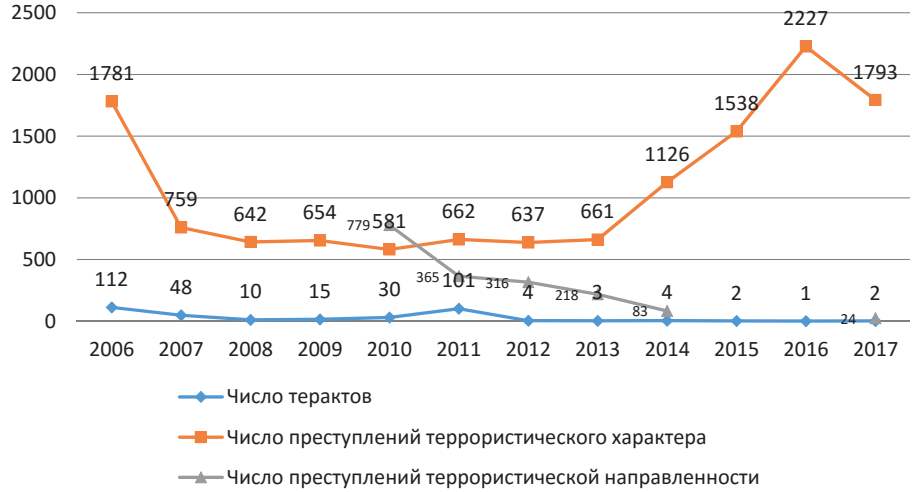


Рис. 2. Количество террористических актов и террористических преступлений в России (Источник: Генеральная прокуратура Российской Федерации. Портал правовой статистики. [Электронный ресурс] URL: http://crimestat.ru/offenses_chart (Дата обращения: 13.05.2019))

Хотя на международном и региональном уровнях разработано около 30 конвенций, договоров и протоколов, направленных на противодействие террористической угрозе, первая и пока единственная консенсусная дефиниция терроризма зафиксирована в Декларации о мерах по ликвидации международного терроризма, принятой Резолюцией №49/60 Генеральной Ассамблеи ООН от 1994 г., согласно которой под терроризмом понимается «преступный акт, направленный на создание обстановки террора среди широкой общественности или конкретных лиц в политических целях»[3].

8 сентября 2006 г. Генеральной Ассамблеей ООН была принята глобальная контртеррористическая стратегия, в соответствии с которой все государства-члены впервые выразили согласие с применением общего стратегического и оперативного подхода к борьбе с терроризмом. Однако в международном сообществе все еще сохраняются глубокие разногласия относительно движущих сил радикализации населения, роли гражданского общества.

Представляется возможным объяснить отсутствие консенсуса по рассматриваемому вопросу следующими двумя причинами:

1. *Разнообразием подходов в рамках национальных законодательств.*

На локальном уровне в рамках национальных дискурсов сложились три подхода: широкий, сбалансированный и узкий.

К странам с «широким» подходом относятся те, в которых определение понятия «терроризм» на законодательном уровне имеет множество отсылок к другим нормативно-правовым актам страны, что придает формулировке весьма запутанный характер.

«Узкий» подход предполагает увязывание этого понятия только с его политической составляющей, следствием чего является отсутствие в законодательстве

специальной криминализации терроризма и связанных с ним деяний. В связи с этим ответственность устанавливается только за те деяния, которые мировым сообществом считаются террористическими.

Сбалансированным считается законодательство стран, принадлежащих к англо-американской правовой семье, поскольку в них предпринята попытка криминализации не только отдельных террористических актов, но террористической деятельности в целом. Несмотря на детальную проработанность, законодательные акты указанных стран не лишены широкого использования отсылок (см.таблицу).

Подходы к определению терроризма на локальном уровне

Национальный дискурс		
«Широкий» подход	«Сбалансированный» подход	«Узкий» подход
Франция, ФРГ, Индия, Испания, Республика Корея	Англо-американская правовая семья	КНДР, Бразилия, Нигер, Вьетнам

Примечание. Источник: Современные международные отношения: Учебник / Под ред. А.В. Торкунова, А.В. Мальгина. М.: Аспект Пресс, 2012. 688 с.

Российское законодательство трудно отнести к одной из вышеперечисленных групп. По своему содержанию оно ближе к сбалансированной, однако имеет качественные отличия от актов, принятых в англосаксонских странах. В частности в российском законе в отличие от законодательств других стран насилие не выступает в качестве отдельного противоправного деяния [2]. Вместо этого применяется термин «идеология насилия» [2].

2. *Сложностью и противоречивостью терроризма как феномена.*

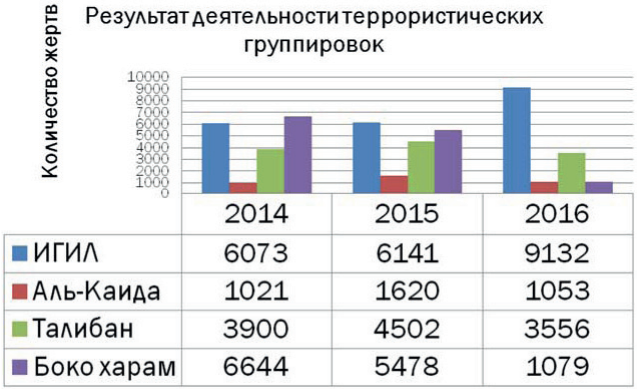
Терроризм как явление не является порождением XXI в. Насилие как форма протеста и метод разрешения политических, социальных и экономических противоречий насчитывает столетия. Вместе с тем, за период своего существования рассматриваемый феномен прошел не один этап эволюции. Так, до середины XX в. террористические преступления, преследующие политические цели, носили эпизодический характер. В последние три десятилетия XX в. терроризм квалифицировался как форма политического экстремизма или форма политического протеста. Так, в период 1960–1970-х гг. терроризм становится инструментом борьбы националистских и ультралевых групп, а начиная с 1990-х гг. XX в. появляются основанные на религиозных доктринах террористические сети, охватывающие не один регион, что позволяет говорить о терроризме как международном феномене.

Анализ наиболее масштабных террористических актов за последние годы показывает, что основными террористическими агентами на современном этапе являются организации радикально исламистского толка или связанные с ними группы. По статистике «Исламское государство», «Аль-Каида», «Талибан» и «Боко харам» ответственны за 78% всех жертв террористических актов в 2014 г., за 74% в 2015 г. и за 59% в 2016 г (см.рис.3) [7].

Международный терроризм эпохи глобализации сложно определить через конкретную сферу его проявления: действуя вне геополитических и геоэкономических рамок, он приобретает системный характер. Признаки международного терроризма также неоднозначны и противоречивы, как и сам феномен. По мнению ряда экспертов [9], наиболее значимыми из них являются:

• политическая мотивировка, позволяющая проводить границу между терроризмом и иными преступными актами, применяющих насилие;

• борьба за власть, при этом субъекты склонны афишировать свои цели;



	2014	2015	2016
ИГИЛ	6073	6141	9132
Аль-Каида	1021	1620	1053
Талибан	3900	4502	3556
Боко харам	6644	5478	1079

Рис. 3. . Результат террористической активности исламистских радикальных организаций

• нанесение ударов по некомбатантам, т.е. представителям гражданского населения, далёким от политики;

• демонстрационный, устрашающий эффект, поскольку истинными целями террористов являются не непосредственные жертвы их акций, а те, кто узнают о происходящем из СМИ.

Примечательно, что несмотря на все выдвигаемые инициативы и применяемые международным сообществом действия терроризм продолжает существовать. К тому же в настоящее время он получил идеологическое обоснование в виде исламизма. Очевидно, что современный терроризм развивается намного быстрее, чем попытки его классифицировать. Кроме того, в условиях глобализации распространение терроризма опережает усилия мирового сообщества по борьбе с этим злом. В связи с этим видится необходимым направить усилия не на последствия, а на первопричины, и, следовательно, определить приоритетные цели и направления, на достижении которых должно сосредоточиться мировое сообщество.

Исходя из особенностей современного терроризма, можно выделить следующие приоритетные направления:

1. Военно-политическое.

Ключевой целью на данном направлении является уменьшение жизненного пространства терроризма как военным путем, так и по средством укрепления центральной власти, ее легитимации.

Примером наиболее последовательного движения к указанной цели являются действия Российской Федерации в Сирии, которые можно представить в виде трех ключевых этапов: 1) разгром основных отрядов «Исламского государства»; 2) запуск Астанинского переговорного процесса; 3) проведение Конгресса сирийского национального диалога в Сочи.

Как отмечают эксперты [5], проведенная военная операция и последующие шаги к политическому урегулированию позволили значительно ослабить позиции «Исламского государства», а также сохранить сирийские государственные институты, такие как правительство и армия, что позволило избежать превращения страны в «несостоявшееся государство» (failedstate) и, следовательно, в плацдарм для дальнейшего распространения террористической угрозы.

2. Экономическое.

Наличие у террористических акторов значительного запаса материальных ресурсов определяет в качестве цели на данном направлении пресечение источников финансирования терроризма. Более 140 миллионов долларов в активах террористов были заморожены приблизительно на 1400 банковских счетах по всему миру, но эксперты говорят, что террористические группы стали все более искусными в ускользании от обнаружения с помощью наличных денег, сложных операций по отмыванию денег или законных подставных компаний [8]. Монетарная практика, укоренившаяся в мусульманской культуре, такая, как пожертвования денежных переводов благотворительным организациям и неформальным центрам, усугубляет трудности в отслеживании финансовых связей террористов. Усилия правоохранительных органов еще больше осложняются тем фактом, что разрушительные нападения могут совершаться при относительно низких затратах.

3. Информационное (идеологическое).

Как отмечает Ю. Хабермас, «спираль насилия начинается со спирали нарушенной коммуникации» [4]. Если нарушенная коммуникация выступает в качестве причины терроризма, то средства коммуникации становятся инструментами осуществления террористической деятельности. Второе название у данного направления объясняется существующим идеологическим вакуумом, нашедшим отражение в современном обществе после распада коммунистического блока. Посредством современных СМИ пустота заполняется идеями создания исламского миропорядка, базирующегося на радикальных трактовках исламской политической мысли.

В данной связи определяющей целью является ослабление информационной связи между массами и исламистами при помощи активизации публичной дипломатии. Возрастание числа интернет-пользователей и уход террористических сетей в киберпространство предопределяет воздействие на общественное мнение при помощи информационных технологий. При этом ключевыми игроками на данном направлении должны быть не только и не столько политические фигуры, а заинтересованные неправительственные организации, СМИ, научные и деловые круги, при объединенных усилиях которых возможно начать борьбу за освобождение «душ и умов» населения от радикальных идей.

Литература

1. Бжезинский В. Великая шахматная доска. Господство Америки и его геостратегические императивы / Пер. с англ. О.Ю. Уральской / Отв. ред.М.В. Егорова. М.: Международные отношения, 2010. 112 с.
2. Противодействие идеологии терроризма и экстремизма в образовательной сфере и молодежной среде: аналитич. доклад / Отв. ред. В.В. Каберник. - М.: МГИМО-Университет, 2015. 54 с.
3. Резолюция Генеральной Ассамблеи ООН 49/60 от 9 декабря 1994 г. [Электронный ресурс] // Организация объединённых наций: сайт организации. [Электронный ресурс]. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N95/768/21/PDF/N9576821.pdf?OpenElement (дата обращения: 2.05.2019).
4. Хабермас Ю. Расколотый Запад / Пер с нем. О.И. Величко и Е.Л. Петренко. М.: Весь мир, 2008. 192 с.
5. Хлебников А.Что Россия выиграла в Сирии? // Российский совет по международным делам, 2016. [Электронный ресурс] URL: httphttps://russiancouncil.ru/analytics-and-comments/analytics/chto-rossiya-vyigrala-v-sirii/ (Дата обращения: 13.05.2019).
6. Global Terrorism Index 2017: Measuring and understanding the impact of terrorism // Institute for Economics and Peace, 2017 [Электронный ресурс] URL: http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf (Дата обращения: 13.05.2019).
7. Global Terrorism Index 2016: Measuring and understanding the impact of terrorism // Institute for Economics and Peace, 2016 [Электронный ресурс] URL: http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf (Дата обращения: 13.05.2019).
8. Kaplan E. Tracking Down Terrorist Financing // Council on Foreign relations, 2006. [Электронный ресурс] URL: https://www.cfr.org/backgrounder/tracking-down-terrorist-financing (Дата обращения: 13.05.2019).
9. Makinda S.M. Global Governance and Terrorism // Global Change, Peace and Security. 2003. Vol. 15. Issue 1. P. 43-58.

Материал поступил в редакцию 21.09.2019 г.

УДК 327

© Ермикова М.С.

© Ermikova M.

АНАЛИЗ ИНТЕРНЕТ-ТЕХНОЛОГИЙ В РОССИЙСКО-УКРАИНСКОЙ ИНФОРМАЦИОННОЙ ВОЙНЕ В 2019 ГОДУ

IANALYSIS OF INTERNET TECHNOLOGIES IN THE RUSSIAN-UKRAINIAN INFORMATION WAR IN 2019

Аннотация. *В статье анализируются интернет-технологии, используемые в российском медиапространстве в условиях информационной войны с Украиной, а также какие каналы получения информации пользуются большим доверием среди населения и почему. Для написания статьи был проведен анализ активности пользователей социальных сетей, связанный с тематикой российско-украинского конфликта: Facebook, Twitter, Вконтакте, Одноклассники в период 15.01.2019 по 15.05.2019 гг. – с помощью системы анализа информации – медиалогии. Исследуются принципы формирования запросов поисковых систем, преимущества голосового поиска информации; рассматриваются манипулятивные методы и приемы, используемые в Сети: вброс, метод создания архитектуры выбора, манипулирование опросами общественного мнения, легализация информации, «окно Овертона», массовый посев фейков, зашумление, «троллинг», дискредитация.*

Abstract. *The author analyzes Internet technologies used in the Russian segment of the Internet in the context of the information war with Ukraine, as well as which channels for obtaining information are widely trusted by the public and why.*

The author analyzed the activity of users of social networks: Facebook, Twitter, Vkontakte, Odnoklassniki in the period from January 15, 2019 to May 15, 2019 using the information analysis system - Medialogia.

In the article, the author explores the principles of search engine queries, the benefits of voice information search; manipulative methods and techniques used on the Web are considered: stuffing, a method of creating a choice architecture, manipulating public opinion polls, "legalizing illegally obtained information", "Overton's window", mass seeding of fakes, noiselessness of the information field, «trolling», discredit.

Ключевые слова. *Интернет-технология, Интернет, поисковая система, социальная сеть, информационная война.*

Key words. *Internet technologie, Internet, search engine, social network, information war.*

Информационная война представляет собой борьбу между государствами и негосударственными акторами с использованием исключительно информационных технологий, базирующихся на производстве, распространении и навязывании информации [8]. На настоящий момент Интернет, обладающий рядом особенностей: анонимности, многовекторности, отсутствии верификации, интерактивности, скорости получения информации — является важнейшей площадкой в российско-украинской информационной войне, способной формировать общественное мнение не только в России и Украине, но и за рубежом.

Для написания статьи был проведен мониторинг активности пользователей социальных сетей, связанный с противостоянием России и Украины: Facebook, Twitter, Вконтакте, Одноклассники в период 15.01.2019 по 15.05.2019 гг. – с помощью системы анализа информации – медиалогии.

Анализируя полученные данные, можно заключить, что по тональности сообщений преобладают нейтральные, на втором месте — негативные и лишь около 2% позитивные. (см.табл.1).

В ряду типов социмедиа: соцсеть, микроблог, блог, форум — наибольшее количество пользователей сосредоточено в соцсетях. Аудитория и вовлеченность соцсети — Вконтакте самая большая среди остальных площадок, на втором месте — Одноклассники, на третьем — Twitter. (см. табл.2, табл.3).

Таблица 1

Тональность сообщений

Тональность сообщений	Всего сообщений	%
Негативные	16583	16,10
Нейтральные	84911	82,43
Позитивные	1520	1,48
Итого	103014	100,0

Таблица 2

Количество сообщений в соцсетях

Тип соцмедиа	Всего сообщений	%
Соцсеть	88130	85,59
Микроблог	9444	9,17
Блог	5133	4,99
Форум	198	0,19
Другое	61	0,06
Итого	102966	100,0

Ермикова Мария Сергеевна *– аспирант факультета политологии, Московский государственный университет имени М.В. Ломоносова, e-mail:ermikova@gmail.com, тел. 8(968)782-94-81.*

Ermikova Maria *– postgraduate student, faculty of political science, M.V. Lomonosov Moscow State University, e-mail: ermikova@gmail.com, tel. 8 (968) 782-94-81.*

Таблица 3

Аудитория и вовлеченность соцсети

Топ-10 площадок	Аудитория	Сообщения	Вовлеченность
ВКонтакте	806425115	44347	185281
Одноклассники	131736586	31514	72286
Twitter	53951964	9444	9660
Facebook	38639882	7498	28243
Instagram	82814501	3260	217592
YouTube	151739105	3226	324787
МирТесен	1463120	1492	1575
LiveJournal	300321	799	2506
Telegram.org	2212711	538	0

Исходя из данных по топ-блогам российской сети можно сделать следующие выводы (см. табл. 4).

Таблица 4

Выводы из данных по топ-блогам российской сети

Топ-10 блогов	Площадка	Аудитория	Сообщения	Вовлеченность
Россия 24 http://www.youtube.com/channel/UC_IEcnNeHc_bwd92Ber-lew	YouTube	2989382	167	3043
Майдан и Антимайдан. Ваша позиция? http://ok.ru/group/52178601377974	Одноклассники	143493	142	0
Новости RT на русском http://vk.com/club40316705	ВКонтакте	1233891	85	369
Анатолий Шарий http://www.youtube.com/channel/UCVPYbobPRzz0SjinWekjUBw	YouTube	2015435	84	30735
http://mirtesen.sputnik.ru http://mirtesen.sputnik.ru	mirtesen.sputnik.ru	2173	70	0
Gunter STuBINGER[2] http://twitter.com/gstubinger	Twitter	1632	69	10
Славяне http://ok.ru/group/57078179758134	Одноклассники	201129	67	441
О главном всерьёз и с юмором http://ok.ru/group/51960235753620	Одноклассники	27068	62	17
Аглая ПУЛИНА http://ok.ru/profile/565861867464	Одноклассники	915	59	340
Владимир Владимирович Путин http://ok.ru/group/51775727206574	Одноклассники	803006	59	0

Самая большая аудитория пользователей (около 3 млн.) сосредоточена на площадке YouTube канала Россия 24, но при этом вовлеченность аудитории всего около 3 тысяч человек, что говорит об активности и заинтересованности ниже среднего значения, однако аудитория в постоянном «контакте» с данным блогом. На другой площадке в Одноклассниках у блога «Майдан и Антимайдан. Ваша позиция?», несмотря на достаточно большую аудиторию (около 143 тысяч) и большое количество сообщений, вовлеченность пользователей равна нулю, то есть блог, по сути, «мертвый», а значит там нет обсуждений, комментариев, репостов и т. п. Хотя тематические площадки на острополитические темы отношений России и Украины при правильном маркетинге могли бы внести свой вклад в информационную борьбу с оппонентами.

А вот блог Анатолия Шарий на площадке YouTube всего лишь при 84 сообщениях за квартал (февраль-май 2019 г.) имеет вовлеченность 30 тысяч пользователей. Анатолий Шарий — украинский журналист, видеоблогер, автор публикаций об организованной преступности на Украине. В 2013 г. создал видеоблог, в котором критикует материалы украинских СМИ, намного реже российских и западных, связанных с Украиной.

Но группа в Одноклассниках, направленная на поддержку В. Путина, при охвате аудитории, равной 800 тыс., имеет лишь 59 сообщений за рассматриваемый период, вовлеченность подписчиков полностью отсутствует. Из чего можно сделать вывод, что подписчики либо неактивные страницы в большом количестве, либо группу ведут очень низкоквалифицированные специалисты, так как через даже фейковые страницы (боты) можно было бы увеличить вовлеченность аудитории, состоящий из реальных людей. Хотя с учетом относительно высокой степени доверия к российскому президенту, блог, в котором бы он или пресс-секретарь транслировали бы официальные заявления с личным отношением к политическим событиям (санкции, обвинения России в аннексии Крыма, поддержки самопровоглашенных республик ЛНР и ДНР, дело Скрипалей,

«Панамское досье» и т. п.), был бы очень популярным.

Фонд общественного мнения опубликовал исследование, посвященное источникам новостей и доверию к СМИ за 2010-2019 гг. [1]. Доверие к новостным телепередачам среди респондентов стало ощутимо меньше: еще в 2010 г. 87% населения получало информацию благодаря телевидению, но уже к 2019 г. – 71%. Снизились доверие и интерес к печатным СМИ: в 2010 г.– 21% респондентов пользовались этим каналом информации, в 2019 г. всего лишь – 12%. К новостным же сайтам в Интернете, наоборот, интерес сильно возрос: в 2010 г. к ним обращались всего 13%, а в 2019 г. – 44%; а также увеличилась степень заинтересованности социальными сетями и форумами – с 4% до 19%.

Можно предположить, что у населения появилась необходимость в самостоятельном отборе интересующих новостей, а также уверенности в истинности информации, в ее альтернативности, возникла потребность в формировании собственного мнения, избегания манипулирования.

Каковы же характеристики активных интернет-пользователей? Доля населения пользователей Интернета в возрасте 18-30 лет – 57% предпочитает получать информацию через новостные сайты, 38% из социальных сетей, блогов, форумов. Также к активным интернет-пользователям относится возрастная группа 31-45 лет – 55%, 20% из них использует и социальные сети; чуть менее активно пользуется сетью группа 46–60 лет – 43% и 17% соответственно, но именно среди нее 80% респондентов отдают предпочтение телевидению, а значит, наиболее восприимчивы для официальной правительственной позиции на общественно-политические процессы. Самый же большой процент среди населения, читающего прессу (12%), это группа людей старше 60 лет – 25%.

Среди пользователей новостных сайтов 59% имеют высшее образование, а вот среди пользователей форумов, блогов, социальных сетей всего 25%.

Когда респондентам предложили выбрать, каким источникам информации они доверяют больше всего, наибольшие показатели достались телевидению — 30% от всего населения, 50% из них это люди за 60 лет, меньше всего TV доверяет группа от 18 до 30 – 23%, это группа незначительно больше доверяет новостным сайтам и социальным медиа: 25% и 20% соответственно.

Всего 26% опрошенных готовы отказаться от телевидения в пользу другого источника информации, а 60% респондентов полностью исключают такую возможность. При этом всего у 14% населения не вызывают сомнения новости телевизионных каналов.

Интересна информация, связанная с вопросом, какие источники обычно используют 58% респондентов, получающие новости в Интернете. 42% ответили, что читают новости в поисковиках Яндекс, Mail.ru, Рамблер, Google или переходят через них по ссылкам. А это означает, что относительное большинство из этой группы не сами формируют запрос на получение конкретных новостей на определенных новостных сайтах с аналитикой автора статьи, например, или официальными заявлениями политических лидеров, а то, что им выдает поисковая система в ТОПе.

Вывести свой сайт в ТОП – это главная задача владельцев сайтов, так как высокие позиции в выдаче обеспечивают трафик и, как следствие, хорошую конверсию. Чем выше позиция сайта при выдаче результатов поиска/запроса, тем лучше. Пользователи открывают сайты, расположенные ниже только в случае, если не нашли то, что искали на первых ресурсах. Чтобы пробиться в ТОП поисковой системы раньше владельцу сайта приходилось работать с семантикой, структурой сайта, закупать рекламу на авторитетных веб-ресурсах. Но в настоящий момент поисковые системы работают по другому принципу: они запоминают те страницы, которые посещают пользователи и в соответствии с этим выдают информацию. Однако это не исключает проблемы, связанной с кликбейтом – термином, описывающим веб-контент, целью которого является получение дохода от онлайн-рекламы в ущерб качеству или точности информации. Когда, несмотря на интересы и хобби пользователя, поисковая система ставит в ТОП контент с «цепляющими» названиями, вызывающими эмоциональный шок и стремление быстрее ознакомиться с информацией, а на самом деле статья может вовсе не соответствовать заголовку или даже служить средством распространения компьютерных вирусов. Из-за этого недостоверная и некачественная информация оказывается в ТОПе куда чаще, чем страницы, связанные с интересами пользователя.

Часто у людей в различных жизненных обстоятельствах просто нет возможности разбираться со сложными сайтами известных и уважаемых новостных порталов и онлайн версиями газет, неадаптированных для входа с мобильных устройств, перебирать различные разделы, чтобы найти нужную информацию. Среди интернет-трендов, наметившихся в 2016 г., можно отметить увеличившееся количество голосовых поисковых запросов. Вне зависимости от того, какой диагональю экрана обладает мобильное устройство, пользователь сегодня предпочитает голосовой ввод запросов.

Чем же обусловлена такая популярность голосового поиска? Дело в том, что ввод голосового запроса происходит в 4 раза быстрее, чем ввод с клавиатуры. Чем меньше действий требуется от человека для решения задачи, тем большую удовлетворенность от процесса он получает.

Дело в том, что ввод голосового запроса происходит в 4 раза быстрее, чем ввод с клавиатуры. Чем меньше действий требуется от человека для решения задачи, тем большую удовлетворенность от процесса он получает. Российская компания — Яндекс смогла уловить новый тренд IT-рынка на создание виртуальных ассистентов, способных распознавать естественную речь, давать ответы на вопросы пользователя и решать прикладные задачи, поэтому создала виртуальный голосовой помощник – «Алису». Важным для разработчиков стало формулирование предложений в текстах с учетом разговорной речи, тщательный анализ ключевых слов в запросах нового типа.

ТОП обсуждений – это рейтинги блогохостингов и разнообразных систем анализа блогов. В них структурирование происходит по количеству комментариев: у какой публикации больше комментариев, та и нахо-

дится в начале списка. Цель – определить наиболее обсуждаемые, а значит, наиболее популярные записи. Их и преподносят пользователю как наиболее актуальные, несмотря на то, что «популярность» может быть создана ботами — фейковыми страницами пользователей. Еще один вариант, это когда структурирование происходит по количеству подписчиков блога. У какого блога больше подписчиков, тот и авторитетнее, но информация, в нем содержащаяся, может быть не достоверной.

Следующие методы касаются непосредственно семантического анализа текстов сообщений Сети.

Метод создания архитектуры выбора — это метод, когда людей ставят перед выбором из нескольких управляемых альтернатив, формируя архитектуру выбора: Вы за или против Майдана? Вы за или против присоединения Крыма к России? Вы поддерживаете инициативу о выдачи российских паспортов жителям ДНР и ЛНР? Очевидно, что это альтернативы, которые приводят к манипуляции, и что если выйти за рамки этого выбора, то откроется больше возможностей того, как относиться к событиям на Украине и как могут складываться дальнейшие события [4].

Манипулирование социологическими исследованиями и опросами — «спираль молчания». Люди, испытывающие страх оказаться в социальной изоляции из-за своего мнения, стремятся примкнуть к большинству [6]. Например, в 2014 г. одной из самых популярных тем было присоединение Крыма к России и мнение граждан по этому поводу. 18 марта 2019 г. ВЦИОМ представил данные исследования, приуроченного к пятилетию присоединения Крыма к России. Во-первых, во всем исследовании это событие обозначается словом — «воссоединение», транслирующее официальную правительственную позицию относительно исторической и правовой обоснованности, слова «аннексия», «присоединение», «вхождение», «оккупация» не встречаются. По полученным данным, 88% опрошенных положительно оценивают воссоединение Крыма с Россией (94% среди людей 60 лет и старше). 21% опрошенных сказали, что теперь можно ездить отдыхать без пересечения границы. 73% россиян считают, что Крым начал развиваться более успешно, когда стал частью Российской Федерации, нежели, когда находился в составе Украины. 9% респондентов, считают, что воссоединение Крыма с Россией отрицательно сказалось на их жизни. Отрицательные последствия опрошенные видят в санкциях против России (4%) и падении уровня жизни россиян (4%). Хотя 29% респондентов не смогли назвать отрицательных последствий, а большинство (70%) наших сограждан утверждают, что воссоединение России и Крыма никак не сказалось на их жизни [2].

В другом исследовании ВЦИОМа данные показывают, что к августу 2016 г., доля россиян, считающих, что Россия должна признать независимость республик, снизилась с 29% до 23%, а доля граждан, предпочитающих соблюдение нейтралитета в вопросе о статусе республик, напротив, выросла с 28 до 38% [3].

Вброс – «резкое заполнение сетевого пространства» какой-либо короткой, но вызывающей широкий спектр эмоций информацией. Например, 20 февраля 2014 г. во время Евромайдана случился обстрел по митингующим и правоохранительным органам Украины. Но самым популярным вбросом стало сообщение в социальных сетях Олеси Жуковской, волонтера Евромайдана, которая написала: «Я умираю». Было показано несколько новостных сюжетов по российскому телевидению, посвященных этому посту, автор которого превратился в настоящего «персонажа» - «жертву Евромайдана». Позднее Олесю прооперировали и спасли ей жизнь, о чем она также сообщила у себя на странице, однако это не подвергалось настолько широкой огласке.

Или другой пример, новость в СМК о том, что в Крыму в 2014 г. появились «вежливые люди» в военной форме, обеспечившие мирный переход полуострова в состав России. Никто из «вежливых» не применял силу, не пользовался огнестрельным оружием и все были очень интеллигентными. То есть фактически военные были в Крыму в тот момент, но не вели себя как бойцы, использовавшие оружие и осуществлявшие захват территории.

Легализация информации – это действие, направленное на то, чтобы получить возможность открыто использовать неправомерно полученную информацию. Показательна в этом плане хакерская группировка «Киберберкут», выступавшая против нового руководства Украины в 2014 г. Хакерская группа занималась публикацией отдельных документов и писем, достоверность которых сложно было проверить. В марте 2014 года стало известно, что «Киберберкут» осуществил ряд атак на веб-ресурсы НАТО и Украины. Хакеры временно заблокировали работу информагентств Liga.net и Unian.net, веб-сайта Андрея Парубия Parubiy.org, западного портала zik.com.ua и ряда других онлайн-ресурсов. Ими были взломаны почтовые ящики региональных отделений партий «Удар» и «Батькивщина» и произведен ряд атак на телефоны украинских политиков.

«Окно Овертона» – суть технологии заключается в том, что требуемый сдвиг мнений в обществе разбивается на несколько этапов: «немыслимо», «радикально», «приемлемо», «разумно», «стандартно», «действующая норма»[7]. Когда против России ввели первые санкции западные страны и США, многие были в состоянии «шока» – в СМК было множество обсуждений, равных вопросу: «как жить дальше», особенно, когда Россия стала использовать ответные санкции. Самым большим страхом среди населения было и есть ожидание войны или изоляции российского государства от западного мира. Но спустя пять лет «санкции» воспринимаются как «норма» - необходимая мера, направленная на обеспечение национальной безопасности. А информационная война с Украиной уже далеко не для всех является противостоянием «братских народов»[5].

Массовый посев фейков – распространение фальшивой информации. Это могут быть фотографии, созданные с помощью графического редактора или ролики, смонтированные в видеоредакторе; персонифицированные страницы известных лиц, созданные от их имени другими людьми; неправдоподобные новости. В государственном секторе были предприняты попытки борьбы с фейками – в марте 2019 г. вступил в силу закон о фейковых новостях, который трактует их как «информацию, распространяемую под видом достоверных

сообщений, создающих угрозу причинения вреда жизни или здоровью граждан, имуществу, угрозу массового нарушения общественного порядка или общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи»[1] .

Зашумление – это тоже массовый посев сообщений «параллельно» важной/серьезной информации. Например, новости о новой пенсионной реформе «утонули» в потоке ежедневных новостей о Сирии и Украине.

Троллинг – это нагнетание участниками общения гнева, конфликта путём скрытого или явного высмеивания, принижения, оскорбления других участников зачастую с нарушением правил сайта и этики сетевого взаимодействия. Выражается в форме агрессивного, издевательского и оскорбительного поведения. Используется как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации. Как вариант, это наполнение комментариев всем, чем угодно, но не тематическими сообщениями. Или сообщениями, которые отталкивают других пользователей от чтения. Ярким примером является волна обсуждений, связанных с личностью новоизбранного президента Украины Владимира Зеленского. Прежде всего «троллинг» касается того, что у нового президента нет политического бэкграунда, кроме главной роли в телесериале «Слуга народа». В комментариях к статьям и самих статьях можно отметить акценты, указывающие на несерьезность происходящего в политической жизни Украины, раз комический актер стал главой государства без развернутой предвыборной программы. Уже заранее в российских СМИ создавался образ президента, агрессивно настроенного против России, ДНР, ЛНР, многих российских и украинских артистов, поддерживающих «аннексию» Крыма, войну в Донбассе, в которой, по мнению В. Зеленского, виновата исключительно «Россия-агрессор».

Дискредитация — действия, направленные на подрыв имиджа и репутации, принижение какого-либо субъекта, подчеркивание негативных и слабых сторон [4]. После президентских выборов на Украине было много сообщений, связанных с тем, что против П. Порошенко будет возбуждено уголовное дело, уже 13 мая 2019 г. генпрокуратура открыла дело по факту давления действующего президента на судей, которые отменили национализацию Приватбанка. То есть бывшего президента Украины созданная им же политическая система власти готова «приговорить» к наказанию. Возможно, впоследствии и другие его законодательные инициативы и политические решения будут негативно переоценены.

Биржи комментариев –это площадки, где можно заказать определенные комментарии в соцсетях, блогах, форумах, сайтах. Процесс распространения необходимых «заказчику» комментариев осуществляется через специально созданные страницы или боты, которые, оставляя лайки, отзывы, увеличивают охват аудитории, тем самым делая ресурс, блог или просто конкретный пост в социальных сетях популярным. Таким образом, имея некоторые финансовые средства, можно создать иллюзию того, что определенная тема активно обсуждается людьми (репостится, комментируется, лайкается, распространяется). А значит — очень важна для пользователей, и заинтересовала их.

Выводы

В период с 2014 по 2019 гг. в информационной войне с Украиной российская коммуникационная стратегия в Интернете развивалась стихийно, в связи с чем сложно выделить главные «месседжи», адресованные пользователям. Связано это с тем, что топ новостей поисковых систем формируется исходя из интересов самих пользователей, их личной истории поиска, что осложняется еще и проблемой кликбейта, поэтому важная и проверенная политическая информация часто «тонет». В этом сегменте необходимо разработать более целенаправленную программу действий, что можно было бы сделать через популяризацию материалов аналитических изданий, авторитетных газет и журналов в Сети, а также через создание тематических групп с регулярно обновляемым контентом, активно вовлекающим аудиторию в процесс политической коммуникации.

Федеральный закон от 18.03.2019 N 31-ФЗ «О внесении изменений в статью 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации» // http://www.consultant.ru URL: http://www.consultant.ru/document/cons_doc_LAW_320401 (дата обращения: 27.03.2019).

Литература

1. Исследование источников новостей и доверия СМИ // fom.ru: Фонд общественного мнения. М., 2019. URL: https://fom.ru/SMI-i-internet/14170 (дата обращения 28.04.2019).

2. Исследование: Крым: пять лет с Россией // wciom.ru: Всероссийский центр изучения общественного мнения. М., 2018. URL: https://wciom.ru/index.php?id=236&uid=9599 (дата обращения: 15.05.2019).

3. Россия и ситуация в Донбассе: мониторинг // wciom.ru: Всероссийский центр изучения общественного мнения. М., 2016. URL: https://wciom.ru/index.php?id=236&uid=115834 (дата обращения 20.04.2019).

4. Володенков С.В. Интернет-коммуникации в глобальном пространстве современного политического управления. М.: Проспект, 2015. 272 с.

5. Джек Т., Райс Э. Маркетинговые войны. Спб.: Питер., 2018. 288 с.

6. Ноэль-Нойман Э. Общественное мнение. Открытие спирали молчания. М.: Прогресс-Академия, Весь Мир, 1996. 352 с.

7. The Overton Window // mackinac.org: Mackinac Center for Public Policy. URL: https://www.mackinac.org/OvertonWindow (дата обращения: 10.05.2019).

8. Расторгуев С.П. Информационная война. Проблемы и модели. Экзистенциальная математика. М.: Гелиос АРВ, 2006. 240 с.

Материал поступил в редакцию 21.09.2019 г.

УДК 327

© Виловатых А.В.

© Vilovatykh A.

НЕКОТОРЫЕ АСПЕКТЫ ПОЛИТИКИ США В ОБЛАСТИ СОВЕРШЕНСТВОВАНИЯ НАЦИОНАЛЬНОЙ СИСТЕМЫ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

SOME ASPECTS OF THE US POLICY ON IMPROVING THE NATIONAL SYSTEM OF INFORMATION WARFARE

Аннотация. *В статье рассмотрены актуальные аспекты политики США по реконфигурации системы информационного противоборства в контексте курса Вашингтона на технологическое лидерство. Приведен подход НАТО к обеспечению кибербезопасности. Предпринята попытка обозначить возможные меры РФ по купированию угроз информационной безопасности.*

Abstract. *The article discusses the current aspects of U.S. information security policy in the context of Washington's course on technological leadership. There is presented NATO's approach to cybersecurity. The author made an attempt to identify possible measures of the Russian Federation to mitigate the information security threats.*

Ключевые слова. *Информационно-психологическое кибербезопасность, Россия.*

Key words. *Technological revolution, information and communication technologies, information and psychological impact, USA, NATO, information security, cybersecurity, Russia.*

В последние годы все более рельефно проступает нелинейность политической динамики, выражающаяся в ее растущей турбулентности и непропорциональности причинно-следственных взаимосвязей. С точки зрения управления политическими процессами основная проблема, порождаемая такой нелинейностью, состоит в снижении возможностей качественного прогноза событий в области международной политики. Российские и зарубежные ученые сходятся во мнении, что складывающаяся ситуация во многом обусловлена происходящей в наше время технологической революцией, которая оказывает воздействие на все сферы жизнедеятельности человека

Знаковой тенденцией современных мирополитических процессов, обусловленных технологической революцией, является усиление в них роли информационного фактора. Если еще в конце двадцатого века инновации в области информационно-коммуникационных технологий (ИКТ) оставались периферийным вопросом в международных взаимодействиях, то в последнее десятилетие использование возможностей Интернета привело к качественно новой их декомпозиции, потому что беспрецедентная доступность информации сочетается со столь же беспрецедентным ее переизбытком. Достижения в сфере ИКТ используются политическими субъектами для анализа экономической, социальной, политической обстановки в отдельных странах и регионах, а также для подготовки общественного мнения к принятию важных политических решений. В Интернете (прежде всего социальных сетях и блогосфере) регулярно апробируются новые методики информационно-психологического воздействия на общественное сознание.

Ситуация усложняется тем обстоятельством, что в мире постоянно увеличивается состав политических акторов, способных применять в том числе военные средства в достижении собственных целей. Участниками военно-политических процессов теперь являются не только государства, но и «акторы вне суверенитета»: военно-политические блоки, спонтанно организованные социальные движения, террористические группировки, националистически или религиозно мотивированные экстремисты и пр. В своей деятельности они также активно пользуются Интернетом (в частности, созданными там социальными сетями) и другими информационными ресурсами. Так, несколько лет назад во многом за счет Twitter-активности была дестабилизирована социально-политическая обстановка в ряде стран Ближнего Востока и Северной Африки, а также на пространстве Содружества Независимых Государств, что привело там не только к смене властных элит, но также к серьезным военно-политическим последствиям [3].

Применение современных ИКТ в политических и военных целях вне пространственных и временных границ ломает шаблонные схемы, присущие прежде политической динамике. Чрезвычайно быстро нарастает процесс политизации виртуального пространства. В решении политических проблем не остается «полутонов». При этом отдельные государства стараются нивелировать собственные достижения в этой области, хотя в последнее время предпринимают принципиально новые усилия по совершенствованию компетенций в информационно-коммуникационной сфере. В частности, американский военно-политический истеблишмент указывает на то, что усиление возможностей от-

Виловатых Анна Вячеславовна *– кандидат политических наук, Российский институт стратегических исследований, E-mail: VilkaVulkan@yandex.ru.*

Vilovatykh Anna *– PhD in political sciences, Russian Institute for Strategic Studeis, E-mail: VilkaVulkan@yandex.ru.*

дельных государств в глобальном информационно-коммуникационном пространстве, скорее всего, еще более ослабит позиции Вашингтона на международной арене.

В принятых в период президентства Д. Трампа доктринальных американских документах киберпространство рассматривается как самостоятельная сфера ведения боевых действий. Например, в опубликованной 19 января 2018 г. Стратегии национальной обороны США отмечается, что в перспективе американское военное ведомство будет уделять приоритетное внимание инвестициям для обеспечения информационной безопасности страны и совершенствовать национальный киберпотенциал с тем, чтобы с его помощью осуществлять весь спектр военных операций. Таким образом, Вашингтон рассматривает силы и средства для решения задач в информационном пространстве в качестве полноценного инструмента защиты американских национальных интересов, наряду с дипломатическими, военными, экономическими, финансовыми, правоохранительными инструментами, и работает над отработкой их согласованного использования государственными ведомствами США [11].

В Национальной киберстратегии (National Cyber Strategy), принятой в сентябре 2018 г., содержится установка на сдерживание противников Соединенных Штатов с опорой на наступательный киберпотенциал, а не усовершенствованные защитные технологии [8]. Ключевая роль в разработке кибервооружения для нужд национальной безопасности возлагается на компанию Northrop Grumman Corporation, с которой ВВС США заключили крупные финансовые контракты. Средства пойдут на разработку, внедрение и обслуживание единой платформы для ведения наступательных, оборонительных и разведывательных операций в киберпространстве [9].

К проведению исследований в области применения ИКТ в военно-политических целях привлечены в основном представители военного и разведывательного сообщества Соединенных Штатов. Осуществлением указанных работ занимаются, в частности, такие американские структуры, как Управление перспективных исследовательских проектов Минобороны (DARPA), Агентство передовых исследований в сфере разведки (IARPA), Научно-исследовательская лаборатория Военно-воздушных сил (AFOSR), Исследовательская лаборатория Сухопутных войск (ARL), Институт поведенческих и социальных наук Сухопутных войск (ARI), Управление НИР Военно-морских сил (ONR) и пр. [2, с. 197-211].

В частности, в октябре 2018 г. в рамках годовой программы Научный совет МО приступил к исследованию перспектив сохранения военного превосходства Америки перед лицом форсированного наращивания вероятными противниками США инновационных возможностей в оборонной сфере. Тогда же заместитель министра обороны по НИОКР Майкл Гриффин (Michael Griffin) указал, что на современном этапе Соединенные Штаты должны найти принципиально новые способы противоборства с их конкурентами на мировой арене. В частности, отмечена необходимость глубокого анализа мотивации оппонентов США, а именно ключевых ценностных установок и интересов зарубежных политических элит, влияющих на принятие государственных решений. Научному совету также начал изучение способов противодействия мероприятиям по оказанию влияния и информационным операциям соперников Соединенных Штатов, включая «борьбу с вражеским нарративом» [12].

Следует также отметить и то обстоятельство, что в конце 2018 г. военно-политическое руководство США приняло решение учредить в составе Совета национальной безопасности новый орган – Управление стратегических нарративов (Office of Strategic Narratives, OSN). Данное ведомство будет подчинено заместителю помощника президента по национальной безопасности по вопросам стратегических коммуникаций, что позволит Управлению самостоятельно выходить на главу государства с предложениями по решению задач в области информационной войны.

Предполагается, что Управление стратегических нарративов займется разработкой эффективных методов противодействия пропагандистским мероприятиям противника: защитой критически важных коммуникационных сетей с использованием всех имеющихся в распоряжении США инструментов; изучением общественного мнения по представляющим интерес для властей аспектам; мониторингом действенности зарубежных акций влияния; популяризацией президентских указов в области внешней и внутренней политики. Кроме того, данный орган будет взаимодействовать с аналогичными структурами стран НАТО в разработке наиболее эффективных методов борьбы с «пропагандой вероятных противников. В целом, по прогнозам американских военных экспертов, указанная структура позволит повысить информационную безопасность Соединенных Штатов, так как по своей эффективности должна превзойти Информационное агентство США (United States Information Agency, USIA), существовавшее в 1953-1999 гг. [9].

Таким образом, в стремлении купировать имеющиеся «окна уязвимости» в национальной системе информационного противоборства от внешних угроз прослеживается активизация усилий соответствующих американских структур по ее совершенствованию. МО США объясняет свою концепцию «упреждающей защиты» тем, что кибератаки якобы уже стали неотъемлемой частью современных военных конфликтов и легли в основу документов, определяющих военную стратегию противников Вашингтона. Между тем приоритетность наступательного подхода к обеспечению безопасности в киберпространстве навязывается международному сообществу именно Белым домом.

Соответственно, помимо развития собственных сил и средств информационного противоборства, США активно используют соответствующие ресурсы союзников, входящих в Североатлантический альянс. Важную роль в противодействии гибридным угрозам руководство НАТО отводит возможностям в сфере кибербезопасности. В соответствии с «Обязательствами по обеспечению кибероборонны», принятыми на саммите альянса, состоявшегося в Варшаве 2016 г., пред-

усматривается: обеспечение необходимого финансирования профильных программ; развитие взаимодействия между национальными структурами, задействованными в сфере информационных технологий; активизацию обмена данными о киберугрозах; отработку вопросов кибероборонны в ходе мероприятий оперативной и боевой подготовки. При этом киберпространство объявлено новой операционной военной сферой, а вопросы противодействия киберугрозам включены в рутинный процесс оперативного планирования Североатлантического союза. Таким образом, как отмечают специалисты, проблема переведена из области теоретических построений в практическую плоскость и становится частью четкого институционального процесса [4, с. 105-106].

Важно отметить и то обстоятельство, что с 2014 г. кибероборона признается составной частью коллективной обороны Североатлантического союза (признается, что к этой сфере применима ст. 5 Вашингтонского договора). Однако вопрос о выработке критериев, на основании которых Совет НАТО может принять данное решение, остается открытым. Итоговыми документами Варшавского саммита гибкая формулировка закреплена и в отношении гибридных угроз: возможность задействования механизмов коллективной обороны в ответ на «гибридную агрессию» не исключается [6, с. 49-68].

С точки зрения противодействия гибридным угрозам большое значение придается наращиванию возможностей гражданского сектора: обеспечению непрерывного функционирования органов государственного управления и бесперебойной работы важнейших национальных служб; повышению безопасности критически важных объектов инфрастуктуры; оказанию эффективной поддержки ВС со стороны гражданских структур в сферах энергетики, транспорта и связи. Целый ряд докладов, подготовленных в 2016-2017 гг. прибалтийскими и польскими аналитическими центрами, специально посвящен проблеме обеспечения устойчивости (боевой, а также связанной с защищенностью жизненно важных систем государства – социальной, политической, экономической и технологической) (resilience; forward resilience) [1].

Следует подчеркнуть, что обеспечение устойчивости и формирование действенного потенциала в сфере кибербезопасности (наряду с развитием национальной территориальной обороны) рассматриваются руководством альянса в качестве важнейших составляющих модели сдерживания недопущением/разубеждением (deterrence by denial). Фактически за так называемой стратегией сдерживания, например, выстраиваемой военно-политическим блоком на своем восточном фланге, просматривается стремление к проведению политики «активной обороны», имеющей выраженное наступательное измерение, в том числе за счет использования гибридных методов противоборства на базе объединенных ресурсов США и НАТО.

В последние годы вод нажимом американцев НАТО взяла курс на разработку новой доктрины кибербезопасности. В рамках ведущихся в блоке актуальных дискуссий главное внимание уделяется тактике совмещения кибероперациий с традиционными военными действиями, а также разграничению понятий оборонительной и наступательной кибероперациий. Обновленная кибердоктрина НАТО может появиться в 2019 г., хотя пока лишь несколько членов блока заявили о готовности к ведению наступательных кибероперациий и внесли соответствующие поправки в национальное законодательство [15].

К реконфигурации системы информационного противоборства США, призванной поспособствовать удержанию доминирующего положения страны на мировой арене, привлечены также влиятельные экспертные структуры Соединенных Штатов. Являясь крупным звеном американской внешнеполитической пропаганды, их представители в большинстве случаев связывают такую необходимость с усиливающимся международным влиянием новых и укрепляющихся центров силы. Например, в конце 2018 г. американский «Центр стратегических и международных исследований» (Center for Strategic and International Studies, CSIS), осуществляющий научно-аналитическую деятельность в том числе по заказу Конгресса и Государственного департамента США, опубликовал доклад под названием «Когнитивный эффект и конфликт государств в киберпространстве» [10].

В указанном документе его автор, вице-президент CSIS Джеймс Льюис (James A. Lewis), отмечает, что «желание конкурентов Вашингтона разрушить ориентированную на США систему международных отношений и достичь регионального доминирования привели к разработке стратегий, тактик и технологий, которые уже в скором будущем могут подорвать американское лидерство на мировой арене». Это осуществляется, по словам Льюиса, прежде всего специализированными СМИ, деятельность которых «подтачивает» основы демократического управления на Западе. Например, в докладе указывается, что центральный элемент российской военной доктрины, отражающий сущность взглядов руководства РФ на войны нового поколения, составляют так называемые операции по формированию у международной общественности определенного когнитивного эффекта, навязыванию чуждого образа мышления оппонентам Соединенных Штатов и странам, придерживающимся так называемой политики военного нейтралитета.

Подобного подхода придерживаются и специалисты американского аналитического центра «Корпорация РЭНД» (RAND Corporation). Эксперты указывают, что якобы проводимые сегодня потенциальными противниками США «активные мероприятия в области информационного противоборства» составляют базу «политической войны против государств демократического Запада». В частности, они отмечают, что якобы ведущаяся в настоящее время политическая война РФ нацелена на дискредитацию образа жизни, ценностей, лидеров западных стран, что является «сутью подхода России к противоборству с основным превосходящим ей по силам соперником» [13].

Следует отметить, что в последние годы на совершенствование американской системы информационного противоборства выделяются все более крупные

финансовые средства. Так, в сентябре 2018 г. по линии Госдепартамента было анонсировано предоставление ассигнований на «противодействие иностранной дезинформации и пропаганде» в объеме около 40 млн долларов. При этом отмечалось, что половина этой суммы будет перечислена на баланс Центра глобального взаимодействия (Global Engagement Center, GEC) из системы Госдепартамента. Остальные средства, как предполагается, будут израсходованы Пентагоном на «внедрение технологий раннего распознавания дезинформации, анализ зарубежной аудитории, наиболее восприимчивой к ее воздействию, а также на развитие эффективного взаимодействия с влиятельными игроками на рынке региональных социальных медиа, неправительственными организациями и журналистами».

Таким образом, в условиях цифровизации социальных и политических процессов Соединенные Штаты предпринимают комплексные меры по совершенствованию национальной системы информационного противоборства. Обеспечение национальной безопасности непосредственно в информационной сфере предполагает курс на повышение эффективности использования потенциала ИКТ в противоборстве со своими вероятными противниками, добиваясь оказания информационно-психологического воздействия на население и политическое руководство отдельных государств, а также их дискредитации на международной арене [7].

Важным аспектом с точки зрения поддержания стратегической стабильности и обеспечения информационной безопасности в международном контексте является привлечения внимания мирового сообщества к наступательному, а не оборонительному подходу США к обеспечению их собственной информационной безопасности в ущерб другим государствам. Причем американский подход чреват рисками и для самих Соединенных Штатов. Ввиду крайней зависимости страны от Интернета она гораздо больше уязвима для кибератак по сравнению с другими государствами. Кроме того, военные специалисты сходятся во мнении о том, что крен в сторону развития наступательных возможностей может привести к отвлечению людских и финансовых ресурсов Вашингтона от решения реальных задач в указанной сфере, что в нынешней ситуации может критичным образом отразиться на безопасности самих США [14].

С учетом предпочтения, отдаваемого Соединенными Штатами превентивным наступательным, а не оборонительным операциям в информационно-коммуникационной среде, риски международной информационной безопасности в этой области, видимо, еще более возрастут. В этих условиях Российской Федерации целесообразно усилить внимание к обеспечению страны оборонным потенциалом, способным гарантировать достижение поставленных в Стратегии национальной безопасности целей, включая создание благоприятных условий для собственного технологического развития в будущем. При этом необходимо совершенствовать российский потенциал «мягкой» силы с целью эффективного противодействия подрывным технологиям и продолжать разработку адекватных мер реагирования на существующие угрозы в невоенной, прежде всего, информационно-гуманитарной области (блогосфере и социальных сетях), а также обеспечивать своевременную подготовку специалистов, по своим компетенциям способных включиться в деятельность в указанной сфере.

Литература

1. Бартош А.А. Конфликты XXI века. Гибридная война и цветная революция: монография / А. А. Бартош. - Москва: Горячая линия-Телеком, 2018. - 282 с.

2. Виловатых А.В. Использование информационно-коммуникационных технологий в военно-политических целях: социально-психологический аспект // Проблемы национальной стратегии. – 2018 № 2 (47). - с. 197-211.

3. Карякин, В. В. Современная геополитическая динамика Ближнего и Среднего Востока [Текст] / В. В. Карякин. - Москва; ИГ "Граница", 2010. - 349 с.

4. Кучинская М.Е. Североатлантический альянс после саммита в Варшаве и перспективы развития отношений Россия–НАТО // Угрозы безопасности России и перспективы отношений с НАТО и США: сб. материалов / Под ред. д-ра экон. наук Г. Г. Тищенко, канд. полит. наук. А. В. Виловатых. М.: РИСИ, 2017 - с.105-106.

5. Марченков В.И., Цибиков В.А. О реализации возможностей сети интернет и программных средств в информационно-пропагандистской работе с военнослужащими / В.И. Марченков, В.А. Цибиков // Мир образования — образование в мире. 2015. № 3 (59).

6. Тищенко Г. Г, Ермаков С.М., Виловатых А.В., Кучинская М.Е., Чижов Д. А, Селянин Я.В. Военная политика новой администрации США // Проблемы национальной стратегии – 2017. – № 6 (45). – с.49-68.

7. Устинкин С.В., Рудаков А.В. Идентичность – объект современного глобального противоборства. – Обозреватель – Observer. 2017. № 9(332). С. 53-61.

8. Department of Defense Cyber Strategy 2018 // US DOD. 2018 URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_(дата обращения: 01.10.2019).

9. How to Stop Losing the Information War // Defense One. 2018 July 26 URL: https://www.defenseone.com/ideas/2018/07/how-stop-losing-information-war/150056/ (дата обращения: 20.08.2019).

10. Lewis James Andrew. Cognitive Effect and State Conflict in Cyberspace // Center for Strategic and International Studies. 2018 September 26 URL: https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace (дата обращения: 20.08.2019).

11. National Security Strategy of the United States of America, 2017 P. 12-13, 31–32. // The White House, December 18, 2017 URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (дата обращения: 02.10.2019).

12. Sherman Jason. Griffin looking beyond guns, bombs to ensure future U.S. military superiority // Inside Defense. 2018 October 31 URL: https://insidedefense.com/inside-pentagon/griffin-looking-beyond-guns-bombs-ensure-future-us-

military-superiority (дата обращения: 21.08.2019).
13. The Growing Need to Focus on Modern Political Warfare // RAND. 2019 URL: https://www.rand.org/pubs/research_briefs/RB10071.html (дата обращения: 12.09.2019).
14. Williams Lauren C. DOD struggles with loss of cyber personnel // FCW. 2018 September 28 URL: https://fcw.com/articles/2018/09/28/cyber-workforce-dod-williams.aspx (дата обращения: 01.10.2019).
15. 6 priorities on Cyber Command's extensive to-do list // Fifth Domain. URL: http://fifthdomain.com/2017/05/09/6-priorities-on-cyber-command039sextensive-to-do-list/ (дата обращения: 01.11.2017).

Материал поступил в редакцию 07.10.2019 г.

II. ИНФОРМАЦИОННЫЙ МЕНЕДЖМЕНТ. УПРАВЛЕНИЕ КОНФЛИКТАМИ И РИСКАМИ

УДК 338.2.

© Малков С.Ю., Билюга С.Э., Мусиева Д.М.

© Malkov S., Bilyuga S., Musieva J.

МЕТОДИКА МЕЖСТРАНОВОЙ ОЦЕНКИ КАЧЕСТВА ЖИЗНИ НА ОСНОВЕ ИНДЕКСА LQI

TECHNIQUE OF INTERCOUNTRY EVALUATION QUALITY OF LIFE INDEX LQI

Аннотация. *В статье приведено описание методики сравнительной оценки качества жизни населения различных стран мира с использованием индекса качества жизни LQI. Проводится подробное описание структуры индекса, процесса подбора показателей. Методология расчета индекса основана на использовании иерархии потребностей А. Маслоу.*

Abstract. *The article presents the methodology for comparatively assessing the quality of life of people around the world using the quality of life index LQI. A detailed description of the structure of the index, the process of picking indicators is carried out. The methodology for calculating the index is based on Abaraham Maslow's Hierarchy of Needs.*

Ключевые слова. *Дезинформация, информационная технология, недостоверная информация, ложь, медиасфера, киберпространство, фасцинация, релятивизация истины, аналитическое чтение, критическое мышление.*

Key words. *Quality of life index, objective and subjective factors, Maslow hierarchy of needs.*

Количественная оценка и сравнительный анализ качества жизни населения в различных странах мира представляет собой актуальную, но и очень сложную задачу. Это обусловлено тем, что до сих пор отсутствует общепринятое понимание того, что включает в себя данное понятие. Описание существующих подходов к оценке качества жизни приведено в работе [1]. По итогам проведенного анализа было выявлено, что используемые методы и вычисляемые на их основе индексы не обеспечивают полноценную оценку качества жизни населения в различных странах. К таковым относятся, например, индексы качества жизни, рассчитанные аналитиками журнала The Economist, International Living Legatum Prosperity Index, а также широко известный индекс человеческого развития (ИЧР). Каждый индекс является уникальным и требует особого рассмотрения, однако общий минус у них всех - это недостаточный учет (как в случае с The Economist, Legatum Prosperity Index), либо отсутствие (в остальных случаях) показателей, учитывающих культурные аспекты жизни людей, их духовное и психологическое состояние. По этой причине имеет место парадоксальная ситуация: по индексу счастья, который составляется на основе социологических опросов населения различных стран мира [2], на первых позициях находятся граждане островных (Вануату, Коста-Рика) либо иных небогатых стран, в то время как развитые государства с высокими экономическими показателями отстают, хотя и являются лидерами в упомянутых выше индексах. Это означает, что для раскрытия полноты представления о качестве жизни необходимо найти дополнительные параметры, которые позволят устранить имеющиеся недочеты в оценках.

С учетом имеющихся подходов к определению качества жизни была предпринята попытка создания интегрированного индекса, учитывающего как субъективные (психологические), так и объективные аспекты его оценки. Создание данного индекса во многом опирается на работу [3]. В качестве методической основы при формировании индекса использовалась идея о том, что качество жизни тем выше, чем в большей степени удовлетворены фундаментальные потребности человека. Для определения фундаментальных потребностей использовалась теория А. Маслоу [4], на основе которой была сформирована «пирамида» потребностей следующего вида:

1. Физиологические потребности.
2. Потребность в безопасности.
3. Любовь, общение, принадлежность к социальной группе.
4. Уважение, признание, престиж.
5. Самовыражение, творчество.
6. Самоактуализация.

Для каждого вида потребностей были выбраны показатели, которые характеризуют степень их удовлетворения (или, напротив, неудовлетворения).

Первым уровнем «пирамиды» являются физио-

Малков Сергей Юрьевич *– доктор технических наук, профессор факультета глобальных процессов, МГУ имени М.В.Ломоносова, e-mail: s@malkov.org;*
Билюга Станислав Эдуардович *– заместитель декана факультета глобальных процессов, МГУ имени М.В.Ломоносова;*
Мусиева Джамиля Маллаевна *– студентка факультета глобальных процессов, МГУ имени М.В.Ломоносова, тел. 8(495)54336-76.*

Malkov Sergey *Yuryevich – doctor of technical sciences, professor of the Faculty of Global Processes, Lomonosov Moscow State University, e-mail: s@malkov.org;*
Bilyuga Stanislav *– Deputy Dean of the Faculty of Global Processes, Lomonosov Moscow State University;*
Musieva Jamilya *– student of the Faculty of Global Processes, Lomonosov Moscow State University, tel. 8 (495) 54336-76.*

логические потребности, которые заключаются в потребности в еде, воде, размножении и т.п., т.е. те, удовлетворение которых необходимо для каждого человека в первую очередь. Для характеристики данной группы потребностей были выбраны показатели младенческой смертности и ожидаемой продолжительности жизни. Будучи важными показателями, они отражают наличие возможности полноценного существования человека. Младенческая смертность была выбрана в качестве показателя ввиду того, что выживаемость новорожденных детей напрямую зависит от условий и качества жизни в стране проживания их родителей, а также от состояния здравоохранения. Ожидаемая продолжительность жизни при рождении, эта характеристика является одной из базовых в современных социально-экономических, демографических исследованиях. Ожидаемая продолжительность жизни при рождении – это среднее число лет новорожденного, которое он должен прожить, если в каждом возрасте условия для сохранения его жизни гипотетически оставались бы такими, какими они были для соответствующей возрастной группы в год его рождения. Она характеризует различные социальные подсистемы – систему здравоохранения, систему социального обеспечения и др., а также оценивает эффективность административного аппарата государства и его социальной политики. Между ожидаемой продолжительностью жизни и индексом качества жизни существует прямая зависимость, в то время как показатель младенческой смертности обратно пропорционален индексу качества жизни. Источником данных для указанных показателей является База данных Всемирного банка, в рамках показателей целей устойчивого развития [5].

Для характеристики второго уровня «пирамиды» - потребности в безопасности – используются следующие показатели: число преднамеренных убийств, а также смертность от загрязнения окружающей среды. Эти показатели отражают наличие угроз жизни человека как от прямых действий других людей, так и от загрязнений окружающей среды. Толковый словарь Ожегова трактует безопасность как «состояние, при котором опасность не угрожает, есть защита от опасности» [6], в оксфордском словаре приводится определение безопасности как «состояние свободы от опасностей и угроз» [7]. Обеспечение безопасности является одной из фундаментальных задач государства, без которого также невозможно существование человека. В данном случае подразумевается наличие безопасности от преднамеренных убийств, а также от смертельной доли загрязнений экологии. Выбор убийств как единственного показателя правонарушений объясняется тем, что в разных странах принят различный подход к определению правонарушений, в то время как количество убийств является универсальным показателем во всех странах независимо от особенностей их законодательства. Еще одной причиной выбора данного показателя является его широкая доступность, в отличие от других правонарушений, данные по которым собирать проблематично. Наряду с этим немаловажную роль играет состояние окружающей среды. Если среда обитания человека загрязнена, государство не старается преодолеть данную проблему, фабрики и заводы ориентируются на максимизацию прибыли без учета концепции устойчивого развития, то в данной стране складывается обстановка, которая неблагоприятно влияет на человека в целом, на его здоровье и на качество жизни. Обеспечение экологической стабильности было провозглашено одной из целей развития тысячелетия, а также продолжает оставаться в составе вновь принятых в 2015 г. целей устойчивого развития. Ввиду того, что оба показателя отражают уровень небезопасности в стране, между ними и индексом качества жизни существует обратная зависимость. Источником статистических данных служит База данных Всемирного банка в рамках показателей целей устойчивого развития [8], а также данные американского Института показателей и оценки здоровья (IHME) [9].

Третий уровень «пирамиды» потребностей включает в себя потребности в любви, в общении. Потребности такого рода лучше всего реализуются в семье, т.е. когда человек вступает в брак и создает семью, где имеются любовь, забота, совместная деятельность и, безусловно, принадлежность к семье. В большинстве случаев разведенные или холостые личности не чувствуют удовлетворенность от образа жизни и стремятся завести семью. Ввиду этого обстоятельства для характеристики данной потребности был выбран показатель зарегистрированных браков и разводов. Источником статистических данных является База данных ООН в части Демографического ежегодника.

Четвертый уровень иерархии потребностей А.Маслоу включает потребность в уважении, в личных достижениях, в признании со стороны окружающих. Качество жизни прямо связано с удовлетворением данной потребности, однако как в международной, так и в национальной статистике сложно найти показатель, который охарактеризовал бы удовлетворение потребности в уважении. Как уже упоминалось выше, признания можно достичь посредством деятельности разного рода. Для характеристики успешности/неуспешности трудовой деятельности человека были выбраны следующие показатели: интенсивность ведения бизнеса, уровень безработицы. Каждому конкретному человеку необходимо иметь уверенность в завтрашнем дне, в реализации своих способностей, в возможности материально обеспечивать себя и свою семью. Реализация этой потребности может быть охарактеризована показателем интенсивность ведения бизнеса. С другой стороны, возможность удовлетворения этой потребности во многом зависит от состояния рынка труда, индикатором которого является уровень безработицы. Безработица является негативным фактором, поэтому между ее уровнем и индексом качества жизни имеет место обратная зависимость. Источниками статистических данных служат База данных Всемирного банка в рамках показателей целей устойчивого развития.

На пятом уровне «пирамиды» А.Маслоу располагается потребность в самовыражении, в творчестве. Показателем того, насколько много людей в обществе за-

нимаются творческой деятельностью, является количество исследователей, а также среднее количество лет обучения, поскольку от уровня образования зависит возможность заниматься творческой деятельностью. Обычно в индексах используется лишь показатель количества лет обучения, что не может полноценно отражать его качество. Последнее представляется довольно сложной задачей на основе имеющихся статистических данных, так как соответствующих показателей либо нет, либо данные имеются не по всем странам. Определение количества исследователей позволяет выявить в целом интерес к познанию среди граждан, а также стремление государства развивать сферу науки. Таким образом, данные показатели в совокупности позволят оценить как уровень образования в государствах, так и его качество. Основным источником для данного показателя являлись статистические данные Всемирного банка в рамках показателей целей устойчивого развития, а также база данных ЮНЕСКО.

На последнем уровне иерархии потребностей мы поместили потребность в самоактуализации. Показателем обеспеченности этой потребности является то, насколько сам человек удовлетворен своей жизнью и считает себя счастливым. Это интегративная и субъективная оценка. Ее отражает так называемый индекс счастья, определяемый на основе социологических опросов представительных выборок населения в различных странах мира [2]. Он характеризует удовлетворенность личной жизнью, социальными отношениями, окружающей средой, положением дел в государстве. Еще одним интегративным показателем, отражающим субъективное восприятие качества жизни, является уровень самоубийств. Это антипоказатель, отражающий состояние социального климата в стране. Данное мнение подтверждается результатами эмпирического исследования Эмиля Дюркгейма [3], который одним из первых установил взаимосвязь между модернизацией и ростом отклоняющегося поведения. Способность общества успешно осуществить модернизацию и при этом справиться с ростом несчастных случаев, преступности, социальной аномии превратилась в значимую предпосылку роста качества жизни. Источником статистических данных для определения указанных показателей являются данные опросов о счастье, размещенные на сайте World Happiness Database (это база данных, разработанная в Роттердамском университете Эразма и основанная на опросах населения более 150 государств [2]), также данные о количестве самоубийств из Базы данных Всемирного банка.

В совокупности все используемые показатели сведены в единую таблицу 1.

Если показатели, предлагаемые для расчета индекса качества жизни, представлены в источниках данных в абсолютных величинах, то они приводятся к удельному виду (на 100 тысяч человек), что дает возможность сравнивать страны по значению каждого из отобранных показателей.

Процесс формирования интегрального индекса качества жизни состоит из следующих последовательных этапов:

1) обезразмеривания и унификации значений показателей;

2) конвертации унифицированных значений на шкалу (2;3);

3) логарифмировании полученных значений;

Таблица 1

Потребности, характеризующие их показатели и источники статистических данных

Потребности	Показатели	Источник данных
Физиологические	Младенческая смертность	База данных Всемирного банка
	Ожидаемая продолжительность жизни	Цели устойчивого развития
Безопасность	Количество преднамеренных убийств на 100 тысяч человек	Управление ООН по наркотикам и преступности
	Смертность от загрязнения окружающей среды	Институт показателей и оценки здоровья (IHME)
Любовь/принадлежность к социальной группе	Количество разводов на 100 тысяч человек	Демографический ежегодник ООН (за 2017 и 2011 гг.)
	Количество зарегистрированных браков на 100 тысяч человек	
Признание/уважение	Количество безработных	База данных ЮНЕСКО
	Количество оплачиваемых рабочих	База данных ЮНЕСКО
	Интенсивность ведения бизнеса	База данных Всемирного банка, цели устойчивого развития
Самовыражение, творчество	Среднее количество лет обучения	База данных Всемирного банка, цели устойчивого развития
	Количество исследователей	База данных Всемирного банка, цели устойчивого развития
Самоактуализация	Индекс счастья	World Happiness Database
	Количество самоубийств на 100 тысяч человек	База данных Всемирного банка

4) определения веса (значимости) каждого показателя в интегральном индексе;

5) формирования интегрального индекса качества жизни на базе мультипликативной свертки: показатели возводятся в степени, соответствующие их весу, с последующим перемножением полученных значений (выбор мультипликативной свертки определен тем обстоятельством, что указанные аспекты качества жизни одинаково важны и не замещают друг друга, то есть отсутствие любого из них не может быть скомпенсировано остальными).

Рассмотрим данные этапы более подробно.

Перед проведением расчетов индекса качества жизни возникает необходимость в унификации значений показателей, потому что они отличаются как единицами измерения, так и разбросом числовых значений. Между значением отдельных показателей и качеством жизни может наблюдаться как прямая, так и обратная зависимость, т.е. для одних показателей наилучшему качеству жизни будет соответствовать наименьшее значение показателя, для других - наибольшее. Унификация показателей представляет собой преобразование их значений, в результате которого их новые значения будут располагаться на отрезке от 0 до 1. Так, единичное значение будет равно лучшему значению показателя по отношению к качеству жизни в рассматриваемой выборке стран, а нулевое равняться худшему. С учетом того, что значения показателей и индекс качества жизни могут быть прямо и обратно пропорциональны друг другу, их унификация проводится с использованием следующей формулы:

• в случае соответствия наилучшего показателя его максимальному значению

$$\tilde{x} = \frac{x - x_{min}}{x_{max} - x_{min}};$$

• в случае соответствия наилучшего показателя его минимальному значению

$$\tilde{x} = \frac{x_{max} - x}{x_{max} - x_{min}},$$

где $\tilde{x}$ - унифицированные данные;

x - исходные данные (значение рассматриваемого показателя для i-й страны);

x_{max} - максимальное значение показателя для рассматриваемой выборки стран;

x_{min} - минимальное значение показателя для рассматриваемой выборки стран.

Унификация шкалы измерений показателей позволяет решить проблему количественной несопоставимости изменений разных переменных, а также проблему разнонаправленности измерений «к лучшему».

В связи с тем, что индекс качества жизни представляет собой мультипликативную свертку, значения показателей целесообразно перенести с интервала (0;1) на интервал (2;3) (путем одновременного увеличения значений всех унифицированных показателей на две единицы) и затем прологарифмировать[1].

Важной проблемой является определение веса (значимости) каждого показателя при вычислении индекса качества жизни. Обычно эти веса определяются на основе социологических исследований или экспертным путем. В данной версии интегрального индекса мы сделали допущение, что удовлетворение всех потребностей «пирамиды» А.Маслоу одинаково важно для людей вне зависимости от того, в какой стране они проживают. С учетом того, что каждая потребность в интегральном индексе представлена одинаковым числом показателей (а именно – двумя показателями), то каждому показателю целесообразно присвоить единичный вес.

Интегральный индекс качества жизни формируется на базе мультипликативной свертки, которая предполагает перемножение всех показателей. Здесь необходимо отметить, что зачастую разработка индекса качества жизни в других работах представляла собой аддитивную свертку, в которой частные показатели складывались. Однако опыт использования таких индексов показал, что аддитивная свертка обладает определенными недостатками. В частности, по смыслу такой свертки, удовлетворение каждой потребности может быть полностью скомпенсировано любой другой потребностью (например, низкий уровень обеспечения безопасности может быть полностью скомпенсирован высоким уровнем удовлетворения физиологических потребностей), что не соответствует действительности. При использовании аддитивной свертки получается, что страна, имеющая наихудшие значения по ряду показателей, может компенсировать это наличием лучших показателей по другим переменным (например, если в стране чрезвычайно высокий уровень загрязнений, однако материальное благосостояние населения находится на высоком уровне, то индекс покажет, что качество жизни в стране высокое). Мультипликативная свертка лишена таких недостатков. При ее использовании высокое качество жизни будет только у той страны, все показатели которой находятся на высоком уровне.

В соответствии с вышесказанным расчёт интегрального индекса качества жизни проводился по следующей формуле:

$$LQI = \tilde{x}_1^{n_1} \times \tilde{x}_2^{n_2} \times \ldots \times \tilde{x}_k^{n_k},$$

где LQI – значение индекса качества жизни в рассматриваемой стране;

k – число показателей, которые определяют уровень качества жизни;

n_k – значение веса показателя[2];

$\tilde{x}_k$ – унифицированное значение показателя после их логарифмирования.

Ниже представлены результаты расчетов индекса качества жизни по изложенной методике.

На рис. 1 изображены результаты расчетов индекса LQI для ряда государств, которые входят в Большую двадцатку (G20), представляющую собой крупнейшие

[1]В принципе возможны и другие способы преобразования унифицированных данных, но, как показали дальнейшие исследования, они слабо влияют на конечные сравнительные оценки качества жизни в различных странах.

[2]Как указывалось выше, в рассматриваемой версии индекса значения весов всех частных показателей принимались равными единице.

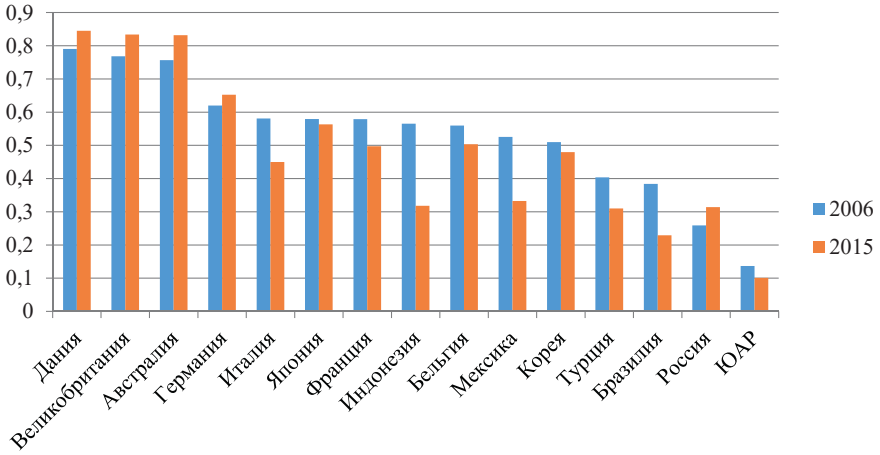


Рис. 1. Значения индекса качества жизни LQI в 2006 и 2015 гг. для стран, входящих в G20

экономики мира и включающую как развитые, так и разивающиеся страны. Рисунок показывает, что качество жизни в рассматриваемый период времени растет в таких странах, как Дания, Великобритания, Австралия, Германия, Россия, а в таких странах, как Италия, Япония, Франция, Индонезия, Бельгия, Мексика, Юж-

Таблица 2

Рейтинг стран по индексу качества жизни за 2006 г.

Страны	Место в рейтинге	Страны	Место в рейтинге
Великобритания	1	Коста Рика	30
Новая Зеландия	2	Чили	31
Норвегия	3	Беларусь	32
Дания	4	Португалия	33
ОАЭ	5	Панама	34
Австралия	6	Латвия	35
Люксембург	7	Хорватия	36
Украина	8	Уругвай	37
Нидерланды	9	Черногория	38
Ирландия	10	Венгрия	39
Швейцария	11	Тунис	40
Швеция	12	Турция	41
Испания	13	Бразилия	42
Финляндия	14	Армения	43
Германия	15	Филиппины	44
Италия	16	Молдавия	45
Япония	17	Болгария	46
Франция	18	Литва	47
Индонезия	19	Азербайджан	48
Бельгия	20	Таджикистан	49
Австрия	21	Киргизия	50
Чехия	22	Македония	51
Словения	23	Сербия	52
Эстония	24	Казахстан	53
Мексика	25	Румыния	54
Греция	26	Босния и Герцеговина	55
Польша	27	**Россия**	56
Южная Корея	28	Гватемала	57
Словакия	29	ЮАР	58

Таблица 3

Рейтинг стран по индексу качества жизни за 2015 г.

Страны	Место в рейтинге	Страны	Место в рейтинге
Дания	1	Испания	30
Великобритания	2	Хорватия	31
Австралия	3	Черногория	32
ОАЭ	4	Венгрия	33
Новая Зеландия	5	Панама	34
Норвегия	6	Коста Рика	35
Люксембург	7	Молдавия	36
Швеция	8	Уругвай	37
Швейцария	9	Мексика	38
Ирландия	10	Сербия	39
Нидерланды	11	Литва	40
Эстония	12	Индонезия	41
Германия	13	Казахстан	42
Финляндия	14	Армения	43
Чехия	15	**Россия**	44
Япония	16	Турция	45
Австрия	17	Азербайджан	46
Беларусь	18	Греция	47
Словения	19	Таджикистан	48
Бельгия	20	Тунис	49
Чили	21	Украина	50
Франция	22	Македония	51
Южная Корея	23	Филиппины	52
Словакия	24	Киргизия	53
Польша	25	Румыния	54
Латвия	26	Босния и Герцеговина	55
Италия	27	Бразилия	56
Португалия	28	Гватемала	57
Болгария	29	ЮАР	58

ная Корея, Турция, Бразилия и ЮАР – снижается.

На основе расчетов индекса *LQI* можно составить рейтинг стран мира по качеству жизни. Этот рейтинг для 2006 и 2015 гг. представлен в табл. 2 и табл. 3 соответственно (расчет рейтинга проведен для стран, по которым имеются необходимые для вычислений статистические данные).

Видно, что место в рейтинге ряда стран за рассматриваемый период поднялось (например, Эстония, Чехия, Чили, Южная Корея, Словакия, Латвия, Болгария, Сербия, Россия), а ряда других стран опустилось (например, Италия, Испания, Мескика, Индонезия, Турция, Греция, Украина, Филиппины, Киргизия, Босния и Герцеговина, Бразилия).

Индекс позволяет выяснить, изменение каких именно показателей привело к повышению или понижению общего рейтинга рассматриваемой страны. Например, подъем рейтинга России по индексу качества жизни с 56 на 44 место за 10 лет связан с ростом таких показателей, как ожидаемая продолжительность жизни и индекс счастья, а также со снижением таких показателей, как уровень безработицы, число преднамеренных убийств, число самоубийств.

На рис. 2, рис. 3 и рис. 4 приведены данные по сопоставлению рейтингов, полученных на основе разработанного индекса LQI и индекса ИЧР [10], индекса журанала The Economist [11], а также индекса процветания Института Легатум [12], соответственно.

Видно, что индекс качества жизни LQI имеет достаточно высокий уровень корреляции с тремя наиболее известными и широко используемыми в международной практике индексами. При этом ближе всего он к индексу процветания Института Легатум (R^2=0,736), при составлении которого используется более 90 показателей и результатов опросов, охватывающих разные стороны жизни населения[1].

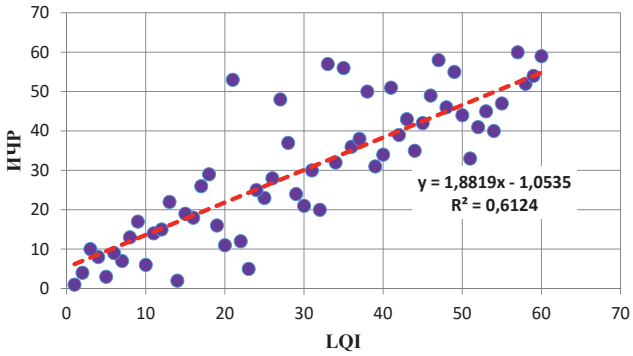


Рис. 2. Корреляционная диаграмма рейтингов стран, полученных на основе индекса *LQI* и индекса человеческого развития

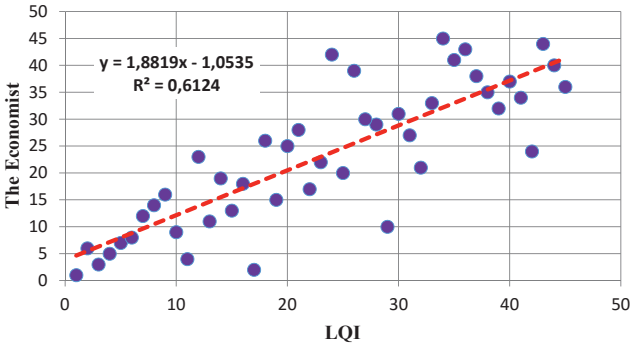


Рис. 3. Корреляционная диаграмма рейтингов стран, полученных на основе индекса *LQI* и индекса журанала The Economist

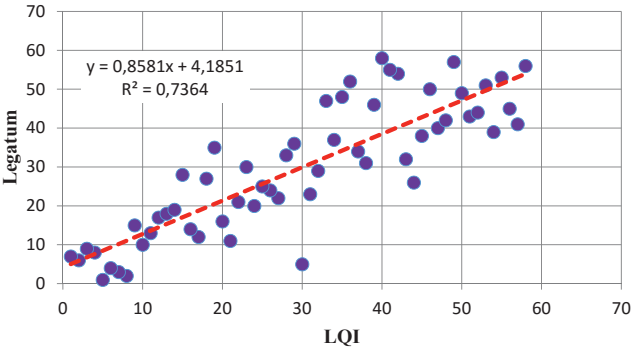


Рис. 4. Корреляционная диаграмма рейтингов стран, полученных на основе индекса *LQI* и индекса процветания Института Легатум

Таким образом, в данной статье приведено обоснование методики сравнительной оценки качества жизни населения различных стран мира. Методика основана на расчете инрегрального индекса LQI, учитывающего как объективные, так и субъективные факторы. Проведено сравнение рейтингов стран, составленными на основе индекса LQI, с рейтингами, составленными на основе других индексов. Анализ результатов сравнительного исследования качества жизни населения в различных странах мира, проведенного с использованием описанной методики, будет представлен в следующей статье.

[1]В отличие от индекса процветания Легатум индекс ИЧР включает в себя лишь три показателя, что, как нам кажется, явно недостаточно для оценки качества жизни. Индекс журнала The Economist использует более широкий набор показателей, однако он весьма специфический, например, в него входят данные о посещаемости церкви, членство в профсоюзах, значения широты анализируемой страны и т.п.

Литература

1. Мусиева Д.М. Понятие "качество жизни" и подходы к его определению // Информационные войны, 2019, №3(51), с.16-20.

2. Veenhoven, R. Happiness in Nations. World Database of Happiness, Erasmus University Rotterdam, The Netherlands / [Электронный ресурс] URL: http://worlddatabaseofhappiness.eur.nl/hap_nat/nat_fp.php?mode=1 (Дата обращения: 21.01.2019).

3. Малков С.Ю., Любовикова Д.О. Индекс качества жизни как показатель развития общества и государства // Информационные войны. — 2014. — № 2(30). − С. 48–52.

4. Maslow A.H. Motivation and Personality. 2nd ed. New York: Harper and Row, 1970.

5. The World Bank Datacatalog. / [Электронный ресурс] URL: https://datacatalog.worldbank.org/dataset/sustainable-development-goals (дата обращения: 20.01.2019).
6. Ожегов С.И. Толковый словарь русского языка: 10 000 слов, терминов и фразеологических выражений / С.И. Ожегов ; под ред. Л. И. Скворцова. - 26-е изд., испр. и доп. - М. : Оникс [и др.], 2009.
7. Oxford living Dictionary / [Электронный ресурс] URL: https://en.oxforddictionaries.com/definition/security (дата обращения: 20.01.2019).
8. The World Bank Datacatalog / [Электронный ресурс] URL: https://datacatalog.worldbank.org/dataset/sustainable-development-goals (Дата обращения: 20.01.2019).
9. Институт показателей и оценки здоровья, (IHME)/ [Электронный ресурс] URL: http://www.healthdata.org/ (Дата обращения: 20.01.2019).
10. Доклады о развитии человеческого потенциала / [Электронный ресурс] URL: http://hdr.undp.org/(Дата обращения: 20.08.2019).
11. Рейтинг качества жизни в странах мира / [Электронный ресурс] URL: https://gtmarket.ru/ratings/quality-of-life-index/info / (Дата обращения: 20.08.2019).
12. Рейтинг стран мира по уровню процветания / [Электронный ресурс] URL: https://gtmarket.ru/ratings/legatum-prosperity-index/info / (Дата обращения: 20.08.2019).

Материал поступил в редакцию 17.09.2019 г.

УДК 327

© Виловатых А.В., Хряпин А.Л.
© Vilovatykh A., Khryapin A.

СОВРЕМЕННЫЕ РАЗРАБОТКИ В ОБЛАСТИ СОЦИАЛЬНОГО УПРАВЛЕНИЯ: ОПЫТ СОЕДИНЕННЫХ ШТАТОВ АМЕРИКИ

MODERN STUDIES IN THE FIELD OF SOCIAL MANIPULATION: EXPERIENCE OF THE UNITED STATES OF AMERICA

Аннотация. *В статье проанализированы некоторые достижения американских ученых по управлению социальным поведением в условиях цифровой среды. Представлен обзор разработанных в США информационно-аналитических платформ в сфере мониторинга и моделирования социально-политического пространства. Предпринята попытка дать тематическую картину ведущихся в Вашингтоне исследований в области технологий социального управления.*

Abstract. *The authors analyzed some achievements of American scientists in the field of social behavior manipulation in the digital environment. There is also considered analytical platforms of monitoring and modeling social and political space. The authors made an attempt to give a thematic picture of the ongoing research in USA in the field of social manipulation.*

Ключевые слова. *Военный конфликт, технологическая революция, общество, информационно-коммуникационная технология, информационно-психологическое воздействие, информационная безопасность.*

Key words. *Military conflict, technological revolution, society, information and communication technologies, information and psychological impact, information security.*

Информационно-коммуникационная сеть интернет, в особенности блогосфера и социальные сети, является, по сути, глобальным поведенческим архивом. Там накапливается информация о привычках, предпочтениях, поступках и местоположении людей. Благодаря доступу к таким данным государственные элиты способны управлять социально-политическими процессами более эффективным образом, чем методами прямого воздействия. Практическим результатом такого непрямого управления являются информационные операции, проводимые на базе объединенных ресурсов США и государств-членов Североатлантического альянса.

Разработка инструментария будущих войн «нового типа» стала для Вашингтона основной задачей, согласно реализуемой с 2015 г. Третьей инициативой оборонных инноваций (Defense Innovation Initiative). По замыслу разработчиков данной концепции, все высокие технологии в социальной, когнитивной, организационной сферах получили двойное назначение. Одновременно была поставлена задача максимально эффективно использовать преимущества Америки в таких областях знаний, как большие данные (Big Data), робототехника, синтетическая биология, исследования человеческого мозга, управление социальными массами и пр. Конечная цель сформулирована просто: к 2030 г. в Соединенных Штатах должна быть создана на основе уникальных технологий такая система вооружений, которую ни одна страна в мире не сможет скопировать и тем более применить [6].

Администрация Д. Трампа поддерживает реализацию инициатив, изложенных в указанном документе. Основные исследования в области управления большими социальными массами ведутся в Управлении перспективных исследовательских проектов Минобороны (DARPA), Агентстве передовых исследований в сфере разведки (IARPA), Научно-исследовательской лаборатории ВВС (AFOSR), Институте поведенческих и социальных наук Сухопутных войск (ARI), Центре прикладного интеллекта и когнитивных наук МО. Широкую деятельность в указанном направлении ведут экспертно-аналитические учреждения, в частности близкий к Пентагону исследовательский центр RAND, Массачусетсский технологический институт, Институт Санта-Фе («Институт критической сложности») и пр.

Так, Управление перспективных исследований Минобороны США, призванное обеспечить сохранение технологического превосходства американских вооруженных сил (ВС), финансирует программы по исследованию потенциала социальных сетей. Например, в развернутом проекте Социальные медиа в стратегической коммуникации (Social Media in Strategic Communication, SMISC) принимали участие такие компании, как Facebook, Twitter, Pinterest и Kickstarter. В рамках организованных экспериментов анализировалась активность пользователей указанных социальных сетей для построения в перспективе системы свя-

Виловатых Анна Вячеславовна *– кандидат политических наук, Российский институт стратегических исследований, E-mail: VilkaVulkan@yandex.ru;*
Хряпин Александр Леонидович *– доктор военных наук, Военная академия Генерального штаба ВС РФ, E-mail: xal127@yandex.ru.*

Vilovatykh Anna *– PhD in political sciences, Russian Institute for Strategic Studeis, E-mail: VilkaVulkan@yandex.ru;*
Khryapin Alexandr *– doctor in military sciences, Military Academy of the General Staff of the Armed Forces of the Russian Federation, Moskow, E-mail: xal127@yandex.ru.*

зей между людьми. Посредством манипулирования новостными потоками изучались индивидуальные процессы восприятия информации. По каждому пользователю сети был составлен профиль, отражающий порядка 150 характеристик с целью дальнейшего конструирования механизма распространения в интернете необходимых потенциальному заказчику сведений. Как отмечают в DARPA, одной из целей данной программы является разработка инструментов защиты американских граждан от дезинформации в рамках национальных интересов США. Однако, судя по всему, подобные проекты реализуются с целью выявления потенциала социальных сетей как пространства для ведения проправительственной пропаганды.

Следует также отметить, что DARPA также активно выделяет гранты на разработку новых биометрических технологий. Это производится с целью изучения поведения личности, для чего применяются биометрические методы автоматической идентификации, основанные на физиологических или поведенческих характеристиках. В частности, именно DARPA предложило новаторскую программу поведенческой биометрии (Behavioral Biometrics). В отличие от традиционных методов идентификации, адаптированных под нужды и особенности компьютеров (пароль и логин), современные позволяют компьютеру опознавать пользователя по его поведению. Агентство предложило именовать этот класс новаторских подходов к опознанию «активной аутентификацией» (Active Authentication).

Указанный набор концепций и моделей «поведенческого анализа» позволяет компьютерным системам без использования сложных паролей самостоятельно распознавать пользователей по тем видам активности, которые строго индивидуальны для обычной деятельности отдельно взятого человека. В качестве примера можно назвать клавиатурный почерк, особенности движений пальцев при работе с мышью, экраном, сенсорной панелью и прочими манипуляторами. По утверждению создателей таких проектов, в дальнейшем их наработки могут быть использованы для создания технологической системы управления групповым и массовым поведением любой размерности [18].

Кроме того, американцы ставят вопрос о расширении возможностей человеческого мышления. Изучению данного аспекта подчинено направление деятельности DARPA, призванное создать устройства, имитирующие работу мозга человека (Brain Initiative, BI) [4]. Эта сфера привлекает представителей Пентагона тем, что кора головного мозга успешно решает задачи распознавания образов в реальном времени и с достаточно низкими энергозатратами. Это, по их мнению, позволит в будущем эффективнее управлять не только пилотируемыми и беспилотными аппаратами, но и поведением человека. В частности, в рамках инициативы Brain запланированы проекты, касающиеся реабилитации повреждений нервной системы, создания искусственного интеллекта, функционирующего подобно человеческому мозгу, и разработки эффективных интерфейсов человек – компьютер, позволяющих осуществить перевод мыслей индивида в цифровую форму и обратно. Как отмечают в DARPA, поставленные перед учеными цели предполагают создание подобных технологий приблизительно к 2020 г.

В последние годы все более выделяются масштабы американских НИОКР по линии «хай–хьюм» (HighHum) – современных гуманитарных технологий, призванных оказывать долгосрочное контекстуальное влияние на широкую совокупность факторов (информационных, социальных, когнитивных и пр.), под воздействием которых формируется система ценностей общества. Важная функция таких технологий – установление устойчивых связей между людьми и побуждение последних к определенным коллективным действиям. Анализ, координация работ по этому направлению и практическое руководство ими осуществляется в основном Агентством передовых исследований в сфере разведки (IARPA). По имеющимся данным, только за 2014-2015 гг. инвестиционные структуры США увеличили вложения в «хай–хьюм» приблизительно в 5…5,5 раз [14].

К исследованию социальных и психологических аспектов человеческого поведения привлечены также американские государственные и венчурные фонды (по зарубежным оценкам, около двадцати, наиболее известный – In-Q-Tel), работающие в связке с образовательными и экспертными структурами, а также национальные лаборатории. В настоящее время функционируют около 25 лабораторий с ежегодным бюджетом порядка 15 млрд долларов и численностью более 60 тысяч сотрудников. Наибольший интерес представляют Лос-Аламосская (LANL), Ливерморская (LLNL) и Сандийская лаборатории с отделениями в Альбукерке и в Ливерморе (SNL). Важными направлениями исследований в данных учреждениях являются моделирование устойчивого развития человеческого общества; моделирование инноваций; управление непредвиденными ситуациями в сложных эволюционных системах; динамические и количественные исследования человеческого поведения и пр. [6].

Все больше задач по разработке новейших технологий социального управления делегируется экспертно-аналитическим структурам и университетам. В частности, в эту деятельность вовлечены Корпорация RAND, Массачусетсский технологический институт (Massachusetts Institute of Technology), Институт Санта-Фе (Santa Fe Institute), Центр прикладного интеллекта и когнитивных наук при Университете Тафтса (Tufts University) и пр. [1].

Например, в междисциплинарном Институте Санта-Фе, расположенном рядом с LANL, ведутся исследования по социально-психологической проблематике, заказчиком которых выступает в основном Пентагон. Так, еще в 2015 г. состоялся семинар американского ученого в области человеческого поведения Алекса Пентланда (Alex Pentland) под названием «Социальная физика» (Social Physics).

Справочно. Алекс Пентланд возглавляет лабораторию динамики человека в Массачусетсском технологическом институте (MIT). Является одним из наиболее влиятельных исследователей в области информационных технологий. Консультирует руководство крупных ТНК и правительство

США. Ему принадлежат слова: «Значение больших данных состоит в том, что они дают информацию о поведении людей, а не об их убеждениях…Мы будем способны предсказывать и управлять поведением рынков и возникновением революций».

В описании к мероприятию содержалась следующая информация: «подробные данные о поведении человека, полученные благодаря социальным сетям, сотовым телефонам, кредитным картам и другим подобным источникам, предоставляют ученым возможность отследить динамику социального научения человека и процесс принятия им решений. В основном для решения таких задач используется потенциал гетерогенных стохастических сетевых моделей. Ученые также могут разработать механизмы стимулирования, которые будут влиять на поведение конкретной личности. Такой подход поможет решить множество современных социально-политических и социально-экономических проблем, в частности, повысить производительность отдельных организаций или даже целых городов. В рамках исследований по данной проблематике будут проводиться эксперименты в масштабах от сотен до миллионов людей» [13]. В качестве применения результатов этой работы указывалось на возможность их применения в целях формирования новых моделей потребления и создания экономических кризисов.

Другим примером можно назвать создание в июне 2015 г. Пентагоном совместно с Инженерной школой Университета Тафтса Центра прикладного интеллекта и когнитивных наук. Он объединил экспертов в области психологии, неврологии, информационных технологий и робототехники с целью определения инновационных подходов к мониторингу мыслительных и физиологических процессов военнослужащих, изучения влияния различных состояний на их поведение в оперативной обстановке и оптимизация этого поведения посредством мультимодальных интерфейсов и роботизированных платформ.

Научные исследования в данной структуре разделены на четыре основные сферы:

а) изучение принципов, обеспечивающих взаимодействие человека и интеллектуальных поддерживающих систем, которые нацелены на оптимизацию мышления и физических возможностей бойцов;

б) исследование возможности управления такими состояниями, как напряжение, тревога, умственные перегрузки, стресс, страх, неуверенность и пр.;

в) изучение выполнения военнослужащими умственных и физических задач в реальной боевой обстановке с учетом соответствующих требований;

г) исследования поведения бойцов в команде [17].

Указанными экспериментами занимается Центр прикладного интеллекта и когнитивных наук, который находится под кураторством агентства DARPA [5].

Таким образом, тематика, масштабы и объемы финансирования лишь некоторых трудов, проводимых военными и экспертно-научными структурами США, демонстрируют намерения Вашингтона обладать эксклюзивными технологиями социального управления, которые могли бы быть применимы для достижения целей национального развития страны.

Результатом исследовательской работы экспертно-научных и военных ведомств Соединенных Штатов в области социального управления является создание информационно-аналитических платформ по мониторингу и моделированию социально-политического пространства в предполагаемом государстве-противнике. В настоящее время Соединенные Штаты все активнее апробируют подобные разработки в сочетании с новейшими технологиями психологической и информационной борьбы.

В частности, интерес представляют компьютерные модели прогнозирования поведением толпы. Так, еще в 2007 г. группа учёных из Университета Аризоны представила промежуточные результаты проекта «Моделирование поведения толпы» (Modeling Crowd Behavior) [10]. Исследователи представили разработку, которая позволяет прогнозировать варианты поведения толпы в различной обстановке и ситуациях. В данной системе используется «агент-центрированная методология», которая предполагает, что агенты (люди) в индивидуальном порядке наделены рядом характеристик (пол, возраст, телосложение, особенности здоровья и язык телодвижений и пр.), а для толпы в целом принимаются во внимание различные коллективные эмоции (спокойствие, паника и пр.). В соответствии с заданными параметрами агенты оценивают поступающую информацию, заражаются «эмоциями толпы», предпринимают различные стратегии коллективной деятельности.

По мнению руководителя проекта, доцента Университета Аризоны Пола Торренса (Paul Torrens), специалиста в таких специфических областях знания, как городская география и кибергеография, методика «Моделирование поведения толпы» может применяться как высокореалистичная среда для создания различных ситуаций, связанных с возникновением опасности для посетителей общественных мест. Как отмечает автор, он также смог ее использовать «для воспроизведения распространяющихся через повседневные контакты заболеваний в толпе». Проект Торренса спонсировался Национальным научным фондом США.

Другим достижением американских специалистов можно считать представленную в 2010 г. разработку главного советника по науке ВВС США Марка Мейберри (Marc Mayberry) под названием «Социальный радар» (Social Radar) [2]. По замыслу автора, данный проект должен стать «системой, которая позволяет видеть то, что происходит в сердцах и умах людей».

Целью разработки «Социальный радар» является раннее обнаружение и прогноз возможности и вариантов политической нестабильности в других государствах. Мейберри отмечает, что создание данной системы стало возможным благодаря ряду обстоятельств:

- насыщению информационного пространства структурированной и неструктурированной информацией, созданию программных продуктов, обеспечивающих эффективный поиск, мониторинг, кластеризацию и агрегацию такой информации;
- созданию «гиперсоциальной сети», включаю-

щей в себя транснациональные сети типа Facebook, LinkedIn и пр., а также различные национальные сети, повсеместному распространению платформы Twitter и соответствующих средств ее мониторинга, извлечения, агрегации и многоконтурной обработки полученной из нее информации;

• экспоненциальному росту аудио- и видеоконтента в сети, происходящему в первую очередь за счет контента, поступающего с различного рода мобильных устройств;

• опережающему росту в интернете данных, полученных от различных подключенных к интернету устройств, от видеокамер до бытовой техники. С учетом привязки практически всех существующих программ и социальных сетей к системе геолокации появляется возможность в режиме реального времени получать картину событий, относящихся не только к определенным странам и социальным группам, но даже к отдельным местам и личностям;

• переводу средств массовой информации в электронный формат, а также процессу оцифровки ранее опубликованных изданий;

• развитию глобальных систем радиоэлектронной разведки (типа ECHELON), позволяющих вести тотальный мониторинг всех телекоммуникационных систем мира;

• созданию и практической отработке систем, позволяющих агрегировать для анализа и синтеза структурированные и неструктурированные информационные потоки в любых форматах и из любых источников (примером такой платформы является система Palantir Technologies).

Таким образом, проект «Социальный радар» базируется на интеграции информационных и когнитивных технологий, последних достижениях прогностики и систем распознавания образов, биометрии, социометрии и ряда других разработок социального знания. В настоящее время, как отмечает куратор проекта, он уже используется военным ведомством США.

Перспективным инструментом анализа социально-политической обстановки является Глобальная база данных событий, языка и настроения (The Global Database of Events, Language, and Tone, GDELT) [15]. Она создана ученым Калевом Литару (Kalev Leetaru) при поддержке Джорджтаунского университета (Georgetown University) и Управления перспективных исследований МО США. Этот проект представляет собой базу данных о мировых политических событиях (более 200 млн событий, восходящих к 1979 г.). Путем анализа открытых источников информации в интернете с использованием компьютерного автоматизированного метода определения отношения индивида к мировым новостям (3 млн узлов, интегрированных с 42 млн информационных ссылок) создан каталог социального поведения и убеждений населения по всему миру. С использованием такого ресурса появилась возможность отследить уровень социально-политической напряженности в заданном регионе мира в текущий момент и с прогнозом на будущее.

В частности, с помощью GDELT был произведен анализ вооруженных конфликтов последних 50 лет. На основе собранной информации аналитики предложили классификацию основных социальных групп: «малочисленная элита» (не более 1…3 %), «социально-политически пассивное население» (75…85 %), «социально-политически активное население» (10…20 %). Показателями, свидетельствующими о вероятности кризиса, специалисты назвали острое недовольство «социально-политически активной части населения» действующей политической элитой и резкое снижение уровня жизни населения после его длительного повышения. Следует также отметить, что система GDELT использовалась для анализа и прогнозирования гражданских выступлений, государственных переворотов и вооруженных конфликтов в период 2014-2016 гг. Эффективность прогнозов составила около 85 %, что для событий социального порядка является большим достижением.

В американском правовом поле функционирует целый ряд компаний и ведомств, предоставляющих в пользование указанные выше системы и непосредственно решающих задачи по обеспечению национальной безопасности в данной области либо обеспечивающих потенциал для их решения. В частности, компания Google при участии венчурного фонда In-Q-Tel и Центрального разведывательного управления США осуществляет проект смыслового анализа и поиска в Интернете информации «Диаграмма знаний» (Knowledge Graph) [8,9], а также поддерживает платформу прогнозной аналитики по выявлению угроз и событий в сфере безопасности под названием «Записанное Будущее» (Recorded Future). Данная платформа вычленяет из контекста веб-страниц имена людей–объектов поиска, упоминаемые ими места и события для того, чтобы анализировать «невидимые связи» этих личностей и прогнозировать их действия в будущем [12].

Другая американская компания Palantir Technologies участвует в совместной с DARPA программе «Тотальная/контртеррористическая осведомленность» (Total/Terrorism Information Awareness, TIA). Ее дочерние проекты (платформы Gothem и Metropolis) также приспособлены для решения задач, поставленных государственными ведомствами Соединенных Штатов и рядом транснациональных корпораций [11].

В целом мониторинг программ исследований, проводимых в экспертно-аналитических учреждениях США, позволяет сделать выводы об общей картине применения достижений социального управления для нужд национальной безопасности. Лапидарный перечень их разработок за последние 15 лет включает следующие направления:

а) технологии сбора, хранения, обработки и анализа больших объемов данных (Big Data, Data Mining);

б) визуализацию данных (Data Visualization);

в) современные гуманитарные технологии (HighHum);

г) социокультурную разведку (Sociocultural Behavior Research and Engineering);

д) разведку на основе открытых источников (Open source intelligence, OSINT);

е) работу в социальных сетях (Human Intelligence);

ж) «операции на основе эффектов» (Effects-Based Operations) («операции на основе эффектов» – применение военных и невоенных средств борьбы на всех уровнях протекания конфликта с целью достижения стратегического превосходства над противником);

з) методики анализа информации (Structured Analytic Techniques, SAT).

Таким образом, в экспертно-аналитических и научных учреждениях США не первый год ведутся работы по созданию систем управления групповым и массовым поведением для решения задач, призванных способствовать более надежному обеспечению безопасности страны. Специалисты Пентагона и американские ученые активно работают над разработкой информационно-аналитических платформ по анализу и моделированию социально-политической обстановки. Их все более широкое использование в практике международных отношений позволяет высказать гипотезу о намерении элит Соединенных Штатов не только создать, но и более активно на деле применять технологии управления социальными массами.

Литература

1. A General Agent-Based Model of Social Learning// RAND. 2017. URL: https://www.rand.org/pubs/research_reports/RR1768.html (дата обращения: 10.05.2018).
2. Air Force's Top Brain Wants a 'Social Radar' to 'See Into Hearts and Minds' // Wired. URL: https://www.wired.com/2012/01/social-radar-sees-minds/ (дата обращения: 18.04.2019).
3. Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community // RAND. URL: https://www.rand.org/pubs/research_reports/RR1408.html (дата обращения: 19.04.2019).
4. DARPA and the Brain Initiative // DARPA. URL: https://www.darpa.mil/program/our-research/darpa-and-the-brain-initiative (дата обращения: 18.04.2019).
5. Engineering Humans for War // The Atlantic. URL: https://www.theatlantic.com/international/archive/2015/09/military-technology-pentagon-robots/406786/ (дата обращения: 19.04.2019).
6. Experimental evidence of massive-scale emotional contagion through social networks // PNAS. URL: http://www.pnas.org/content/111/24/8788.full (дата обращения: 19.04.2019).
7. Goodman M. Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It, Doubleday // Studies in Intelligence Vol 59, No. 3. URL: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-3/pdfs/Future-Crimes.pdf (дата обращения: 18.04.2019).
8. IQT Labs // In-Q-Tel, Inc. URL: https://www.iqt.org/labs/ (дата обращения: 19.04.2019).
9. Knowledge Graph // Google. URL: https://www.google.com/intl/es419/insidesearch/features/search/knowledge.html (дата обращения 21.04.2019).
10. Mind of the Mob: The Geosimulation of Crowd Control // Yale Scientific Magazine. URL: http://www.yalescientific.org/2013/05/mind-of-the-mob-the-geosimulation-of-crowd-control/ (дата обращения: 18.04.2019).
11. Palantir Technologies, 2019. URL: http://www.palantir.com/ (дата обращения 21.04.2019).
12. Recorded Future, 2019. URL: https://www.recordedfuture.com/ (дата обращения 15.05.2018).
13. Social Physics // Santa Fe Institute. URL: https://www.santafe.edu/events/social-physics (19.04.2019).
14. Society's Nervous System: Building Effective Government, Energy, and Public Health Systems. A. Pentland in Computer, Vol. 45, No. 1, pp. 31–38.
15. The GDELT Project, 2019. URL: https://www.gdeltproject.org/ (дата обращения: 18.04.2019).
16. US military studied how to influence Twitter users in Darpa-funded research // The Guardian. URL: https://www.theguardian.com/world/2014/jul/08/darpa-social-networks-research-twitter-influence-studies (дата обращения: 18.04.2019).
17. US Army, Tufts team up to advance cognitive science // DefenceTalk. URL: https://www.defencetalk.com/us-army-tufts-team-up-to-advance-cognitive-science-64761/ (дата обращения: 19.04.2019).
18. Waitt T. SecureAuth unveils behavioral biometric technology in partnership with DARPA-endorsed BehavioSec // AST. URL: https://americansecuritytoday.com/secureauth-unveils-behavioral-biometric-technology-in-partnership-with-darpa-endorsed-behaviosec/ (дата обращения: 18.04.2019).

Материал поступил в редакцию 07.10.2019 г.

УДК 070

© Любимова Т.М.

© Liubimova T.

НЕОЛОЖЬ В ОБЩЕСТВЕ ПОСТПРАВДЫ: АКТИВНОСТЬ «FAKE NEWS» В СЕТИ

NEO-FALSE IN POST-TRUTH COMPANY: FAKE NEWS ACTIVITY IN THE NETWORK

Аннотация. *В статье идет речь о новых законодательных инициативах России в области борьбы с недостоверной информацией; рассматривается специфика «fake news» в ракурсе диверсификации терминов и в системе других понятий, связанных с искажением истины; показывается социальная роль «фейков» в обществе «пост-правды» и систематизируются некоторые меры информационной защиты на индивидуальном и общественном уровне.*

Abstract. *The article deals with new legislative initiatives of Russia in the field of combating unreliable information; the specificity of "fake news" is considered from the point of view of the diversification of terms and in the system of other concepts related to the distortion of truth; It shows the social role of "fakes" in the society of "post-truth" and systematizes some information protection measures at the individual and social level.*

Ключевые слова. *Дезинформация, информационная технология, недостоверная информация, ложь, медиасфера, киберпространство, фасцинация, релятивизация истины, аналитическое чтение, критическое мышление.*

Key words. *Misinformation, information technology, unreliable information, lies, the media sphere, cyberspace, fascination, relativization of truth, analytical reading, critical thinking.*

В марте 2019 г. вступили в силу два федеральных закона: Федеральный закон от 18.03. 2019 г. №31-ФЗ «О внесении изменений в статью 15.3 Федерального закона "Об информации, информационных технологиях и о защите информации"», предусматривающий механизм удаления с сайтов недостоверных новостей; и Федеральный закон от 18.03. 2019 г. №27-ФЗ «О внесении изменений в Кодекс РФ об административных правонарушениях», устанавливающий перечень штрафов за распространение недостоверных новостей.

Первый закон окрестили «законом о фейках», причем не только в разговорной речи, но даже на уровне вполне официальном, включая нарратив «Российской газеты» [1], хотя само слово «фейк» в текст закона не попало: объектом правового регулирования обозначена, как и прежнем тексте Федерального закона, «недостоверная общественно значимая информация, распространяемая под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи».

Появление неологизма «фейк» (от англ. «fake» - фальшивый, ложный) логически влечет за собой постановку вопроса о диверсификации терминов, обозначающих поддельную информацию. Контуры этой терминологической структуры намечены в самом тексте закона, где говорится о недопущении «использования новостного агрегатора в целях сокрытия или фальсификации общественно значимых сведений, распространения недостоверной общественно значимой новостной информации под видом достоверных сообщений», то есть по сути вырисовывается триада из лжи (одной из форм которой является умолчание, сокрытие), дезинформации (фальсификации) и манипуляции сознанием (распространения недостоверной информации под видом достоверной).

Постараемся прояснить семантическую оригинальность «фейков» на обширном терминологическом поле среди других понятий, столь же смело «плавающих под пиратским флагом». Понятийный аппарат способов искажения истины в речи включает в себя следующие термины: дезинформацию, пропаганду (агитацию), языковую демагогию, брейнуошинг, суггестию, нейро-лингвистическое программирование, фабрикацию согласия (термин Хомского), одномерное мышление (термин Маркузе), коррупцию языка (термин Болинджера), манипуляцию сознанием [2]. Все они прямо или косвенно взаимосвязаны со словом наиболее общей семантики – «ложь». Традиционно ложь предстает в формах 1) прямой лжи, 2) умолчания, 3) полуправды.

1. Французский социолог А. Моль писал, что СМИ в современном информационном обществе допускают прямую ложь только для того, чтобы по реакции масс уточнить порог восприятия ими фальсификаций и затем снизить уровень лжи ниже этого порога

Любимова Татьяна Михайловна *– доктор философских наук, доцент, профессор, Московский государственный университет им М.В.Ломоносова, тел. 8(919)723-43-32.*

Lyubimova Tatyana *– doctor of philosophy, associate professor, professor, M.V. Lomonosov Moscow State University, tel. 8 (919) 723-43-32;*

[3], то есть сделать ложь "пригодной" для использования потребителями «общества потребления». Однако тенденция, зафиксированная А. Молем в 60-е годы XX века, вряд ли сохраняется в информационных процессах XXI века: ведь если умонастроения западного общества в период «тридцати славных лет» послевоенного восстановления можно было бы обозначить прустовской формулой «в поисках утраченной правды», то в XXI веке медиаобщество вступает в эпоху постправды, как это отмечается в докладе председателя Мюнхенской конференции по безопасности 2017 г. В. Ишингера «Пост-правда, пост-Запад, пост-порядок». В новых условиях прямая ложь приобретает уже не прикладное, а самоценное значение. Более того, в современном мире ложь охватывают все социальное пространство, становясь некоей новой ноосферой, сплавляющей воедино судьбы человечества XXI века и трансформации природы. Это замещение фактической правды ложью в логосфере и в политическом резервуаре, в котором живет современный человек, по-разному осмысляют многие современные исследователи. «Ложь, культивируемая в условиях господства новых медиа, направляется на саму структуру знания о фактах, при этом в обман вводится общество в целом, включая самих лжецов, что чревато абсолютной утратой реальности» [4]. «Особенностью политики XX в. стало то, что ложь перестает быть формой индивидуального высказывания и начинает организовывать политический дискурс как таковой. Ложь становится рамкой, внутри которой политический дискурс себя разворачивает... Происходит своего рода переворачивание фрейма: не ложь существует (как частный момент) внутри политики, а политика реализует себя как систематическая ложь (становится абсолютной рамкой)» [5].

2. Другой формой лжи является умолчание. Этот прием получил еще одно название – «выравнивание», то есть преуменьшение значения важного факта или события. Типологически близок приему умолчания и так называемый метод «барража» – способ отвлечения общественного внимания от какой-либо политической реальности или события. В образной системе "мягкой пропаганды", предложенной А.С. Мироновым, этот прием называется "занижение инфоповода".

3. Еще один известный прием – «полуправда-полуложь» – основан на комбинировании истинной и ложной информации: технология его основана на том, что правда, подобно ракете-носителю, «выводит на орбиту» определенную порцию лжи, соответствующей намерениям лжеца. Если воспользоваться другой когнитивной метафорой, готовится своего рода информационный «бутерброд», один из слоев которого релевантен основной цели воздействия, другой призван обеспечить податливость реципиента к усвоению информации.

На таком обширном семантическом поле, вбирающем в себя полную цветовую палитру лжи (помимо традиционных «черной» и «серой» пропаганды) – от старейшей дезинформации с нюансами идеологической диверсии, всесторонне изученной в работах исследователей советского периода (А.И. Власов, Д.А. Волкогонов, Ю.В. Воронцов, Я.Н. Засурский, Ю.В. Кашлев) и ныне переодевшейся с «информационную диверсию» (например, в протестах «Роснефти» в адрес «Рейтер» [1]) – до «симулякров» постмодерна (Ж Бодрийяр), симулирующих реальность путем подмены ее эрзами и артефактами истории, – термин «фейк» выглядит «осиротевшим». Возникает вопрос, осталась ли на долю этого термина какая-то оригинальная доля семантики, связанной с искажением истины, или это одна из форм, агрессивно вытесняющих исконные формы языка за счет завораживания сознания внешним эффектом (краткостью, западным стандартом и др.). В научной литературе подобные слова определялись как «пустые слова», «слова магической силы» (Г. Лебон), «магически-ритуальные формулы» (Г. Маркузе), «идолы толпы» (Л. Витгенштейн), «слова-ловушки» (Ф. Бретон), «формы-заменители» (С. Брюне), «слова-амебы» (С.Г. Кара-Мурза). «Из науки в идеологию, а затем и в обыденный язык перешли в огромном количестве слова-«амебы», прозрачные, не связанные с контекстом реальной жизни... Они делятся и размножаются, не привлекая к себе внимания – и пожирают старые слова. Они кажутся никак не связанными между собой, но это обманчивое впечатление. Они связаны, как поплавки рыболовной сети – связи и сети не видно, но она ловит, запутывает наше представление о мире... Важный признак этих слов-амеб их кажущаяся "научность". Скажешь коммуникация вместо старого слова общение или эмбарго вместо блокада и твои банальные мысли вроде бы подкрепляются авторитетом науки» [6].

Представляется, однако, что термин «фейк» - не пустая английско-снобистская номинация, что в этом термине сигнификат (понятийное содержание слова) при всей своей неизбежной произвольности максимально адекватен денотату (обозначаемой словом реалии).

Под «фейком» понимается ложная информация, предназначенная для распространения в социальных сетях. Как сказал директор одной из лабораторий информационных систем К. Аберер, «правда – это не что иное, как социальный консенсус» [7]. Вездесущая ложь – это тоже продукт социального консенсуса, который вырабатывается в значительной мере в социальных сетях; они же и привносят «человеческий фактор» в процесс моделирования и распространения недостоверной информации.

Пропущенная через социальные сети недостоверная информация становится фейком, который приобретает следующие характеристики

1. В эпоху ультраинформации и гипер-подключения фейки достигают сверхскоростей. СМИ оказываются «между двух огней»: между жгучей необходимостью досконально проверять информацию до ее опубликования и горячим желанием обойти конкурирующие издания в погоне за сенсационностью. Подогревают

[1]Публикация «Рейтер» является откровенной ложью, цель которой провокация против «Роснефти»//ПАО «НК «Роснефть». Эхо Москвы, 19 апреля 2019г.

процесс производства фейков и пользователи: «граждане часто становятся жертвами fake news, являясь одновременно сообщниками в их распространении» [8]. Эта релейная связь создает неиссякаемый и сверхскоростной новостной поток в рамках «глобальной деревни» (М. Маклюэн), в которую превратился современный мир, где сенсации новостных агентств облетают информационное пространство быстрее, чем сплетни методом «из уст в уста» передавались в иные времена по всему поселку.

2. Тотальность фейкового пространства. Массачусетский технологический институт изучил 126 тысяч информаций, которыми обменивались в «Твиттере» с 2006 по 2017 гг. 3 млн человек, и пришел к безапелляционным выводам: у фейков на 70% больше шансов для публичного обмена в сети, чем у достоверной информации, которая циркулирует в коммуникационном пространстве в шесть раз медленнее, чем недостоверная [9].

Продукты ложного сознания пролиферируют и метастазируют, создавая гигантскую медиасферу всеобщего обмана. Эта лого- и медиасфера «манкуртовой шапочкой» сдавливает массовое сознание, не способное более диагностировать симптомы и синдромы лжи, контагиозность которой достигает и самих лжецов. Ложь могла бы сомкнуться беспросветным куполом над человечеством, однако новая общественная тенденция породила и контртенденцию. В целях самозащиты человечество создало новую профессию «fact-chechers» – специалисты по проверке фактов; кроме того, каждое солидное зарубежное издание имеет свою службу проверки информации; гиганты «мировой паутины», такие как «Гугл» и «Фейсбук» затрачивают миллионы долларов на борьбу с fake news.

3. «Безразмерность» и многофункциональность фейков. В сети можно встретить фейки любого «калибра» от невинной игры до грандиозного обмана, способного менять судьбы мира. Немало сетевых мистификаций имеют самоценный характер: мистификации ради мистификации. К такого рода минифейкам относится, например, запущенная в сеть информация о том, что американский президент Трамп, выступая в НАТО, сообщил, что его отец немец; или о том, что бывший президент Франции Саркози сделал себе рок-татуировку. Фейки «среднего калибра» создаются для того, чтобы локально посеять панику, нанести медийный урон или моральный вред, запустить финансовые махинации, создать помехи для следствия, участвовать в лоббизме, продвигать в соцсетях товары и услуги, завязать успешные знакомства, выдавая себя за другого и т.д. Фейки «крупного калибра» участвуют в большой геополитической игре. Например, госсекретарь США К. Пауэлл, выступая в 2003 г. перед Советом Безопасности ООН, заявил, что «Ирак упорно пытается обрести оружие массового поражения». В 2004 г. Пауэлл признался, что он опирался на информацию, предоставленную ЦРУ, однако источники были неверными и неточными. Совет Безопасности ООН тогда не санкционировал применение военных сил против Ирака, война тем не менее началась, длилась почти 9 лет, обострила религиозные конфликты, генерирующие акты терроризма. Война привела к потерям, которые для США оцениваются в 4,5 тысячи человек, а потери среди иракского гражданского населения столь велики, что даже не подсчитываются с точностью. Таким образом, США запустили военную кампанию, спровоцированную фейком, придуманным беженцем из Ирака, который признался позднее, что сочинил историю про оружие массового поражения, чтобы освободить Ирак от Садаама Хусейна.

На фоне разномасштабности фейков нарастает и многофункциональность мистифицирующих практик: «Это может быть коммуникативная игра с потребителем, где оба участника одинаково понимают шуточную функцию мистификации; это могут быть стратегии персонифицированной дискредитации; наконец, это могут быть цели активизации гражданского общества, построенные на провокационном воздействии» [10].

4. Провокационное воздействие и определяет провокационный характер фейков, который становится их метауровневой детерминантой. Провокационный характер фейков во многом обусловлен наложением в медиасфере и киберпространстве логосферы (вербальных знаков), эйдосферы (графических и живописных форм) и акусферы (звуковых форм). Если печатный текст склонен представать для читателя «спящим», и его еще надо «разбудить», иногда даже расшифровать с использованием инструментария герменевтики как науки об истолковании смыслов текста, то сетевое и/или масс-медийное сообщение «пробуждает» адресата, его будоражит, активно используя невербальные формы воздействия. Визуальные и акустические образы в своем комбинаторном, синергетическом воздействии создают эффект фасцинации, то есть обострения восприятия за счет фоновых воздействий. Фасцинация ослабляет защитные фильтры адресата и открывает заслоны для внедрения манипуляции. Например, в книге Ж.-Л. Вейссберга «Присутствие на дистанции» речь идет о манипуляции сознанием в аудиовизуальных СМИ, которая связана с тягой превратить информацию в околдовывающий спектакль, призывающий к чувственному в нем участию, - в «спектакт», мифологизирующий сознание зрителя в измерениях «логосферы /графосферы/ видеосферы» [11]. Этот призыв к чувственному участию в информации независимо от ее контента и есть не что иное, как провокация.

Провокационный характер видеороликов с фейковыми сюжетами может быть столь мощным, что полиция возбуждает уголовное дело по статье «угроза или насилие», как это было в преддверии президентских выборов на Украине, когда в сети появилось видеоролик, представляющий, что В. Зеленского сбивает грузовик. Такой же скандальный характер имел и фейк-расправа с оппозиционным российским политиком А. Навальным. 22 декабря 2017 г. в официальных сообществах администрации соцсети появились репосты новости о смерти политика. Сообщество издания «Медуза», которое было источником новости, оказалось ненастоящим, его быстро заблокировали, сами публикации удалили, но запись стала распространяться другими пользователями.

5. На эффект завораживания сознания (эффект фасцинации), направленный на «присоединение аудитории», работают также такие «крутые» технологии фейков, как прикол, розыгрыш, мистификация. Приколы и розыгрыши устраиваются с использованием технологии мелких хитростей, которые хорошо изучены журналистами и издателями [12]. Среди «тысячи и одной» хитростей индустрии фейков выделяют такие, как продвижение в маске; узурпация чужой идентичности; манипуляция фактами и образами; потопление пропаганды в непредвзятых фактах; сокрытие ошибок; бегство от преследования. Технология «продвижение в маске» может быть проиллюстрирована уловками сайта «Info Bordeaux», который позиционирует себя как традиционное средство массовой информации, но поддерживается ультраправыми силами. «Узурпация чужой идентичности» демонстрируется на примере деятельности одного интернет-пользователя, который запустил в сеть ложную информацию о том, что Саудовская Аравия оказывает эксклюзивную поддержку Э. Макрону на президентских выборах во Франции, создав для этого двойник сайта бельгийской газеты «Суар» - «lesoir.info»; причем изобретательность хакера достигла такого технического совершенства, что когда пользователи, желая убедиться в достоверности информации, «кликали» по подделке, она перебрасывала их к сайту реально существующей газеты. «Манипуляция фактами и образами» раскрывается на примере фотомонтажей, коллажей, придуманных цитат. В сети стало модно публиковать подлинные, но вырванные из контекста фотографии. Например, любительское видео, снятое в калифорнийской пустыне в декабре 2015 г., было через полгода приурочено к катастрофе с самолетом египетских авиалиний. «Потопление пропаганды в непредвзятых фактах» – это стандартная технология смешения правды и лжи в пользу последней. В пример приводятся ухищрения французского портала ультраправых сил «fdesouche.com», который вполне добросовестно репостирует материалы влиятельных газет, но изредка позволяет себе без проверки и дальнейшего опровержения преподнести пользователям абсолютную фальшь, вроде информации о том, что во Франции «в отелях каждую ночь спят 40 тысяч мигрантов». Технология «сокрытие ошибок» придумана для тех, кто хочет продолжать распространять обман, сохраняя при этом непорочную репутацию. Так, блогер О. Беррюйе нередко публикует непроверенные сенсации (например, конспиративную теорию американца П. Робертса о том, что дирижировало терактом против французского сатирического еженедельника «Шарли Эбдо» американское правительство), которые через некоторое время просто становятся недоступны (500 удаленных статей): фейки успели сделать свое дело, и их можно тихо удалить без опровержения, мотивируя это неактуальностью темы. «Бегство от преследования» предполагает попытки «перевести стрелки» ответственности на какого-нибудь «стрелочника», например, на сайте «Riposte laïque» нашли такую «стрелочницу», которой оказалась одна марокканка, проживающая в Тайланде.

6. Пропущенные через социальные сети фейки «обрастают» человеческим фактором, впитывают в себя субъективность оценок разных пользователей и партикулярность их жизненных позиций и убеждений. Причем структура индивидуального сознания, взаимодействующего с сетью, распадается минимум на три уровня – рациональный, эмоциональный и уровень интенциональных состояний, под которым в современной философии понимается «то свойство мышления (мозга), благодаря которому оно способно репрезентировать другие вещи» [13], то есть ментально-психологические реакции, направленные на объекты внешнего мира.

1. Рациональный уровень индивидуального сознания. Как утверждает французский психолог А. Мукейбер [14], мы видим и слышим нашим мозгом, который является фильтром, определяющим степень пригодности для нас той или иной информации. Для этого мозг использует ментальные модели – эвристики, позволяющие ему решать интеллектуальные задачи упрощенным, экономным путем. «Эвристический путь подразумевает применение эвристического правила, обычно основанного на очевидном значимом признаке (например, на компетентности источника), который виден сразу и снимает необходимость детального анализа сообщения» [15]. Но этот механизм фильтрации, основанный на применении эвристик, нередко дает сбой, ибо наш разум идет не путем объективизации, а путем мотивации. Когда мы знакомимся с новой информацией, мы обычно сопротивляемся тому, что противоречит нашим взглядам, и доверчиво относимся к тому, с чем заведомо согласны. «Мы преднамеренно избегаем встречи с информацией, не согласующейся с нашими установками; не желая, чтобы сообщения, несущие такую информацию, вызвали в нас диссонанс, мы стараемся вовсе ее не слышать» [16]. Чтобы снять когнитивный диссонанс, наш мозг по-новому обустраивает действительность. Что касается фейков, то, по мысли А. Мукейбера, их контент относится не к области неведения, а к области иллюзии знания. Часто мы где-то уже слышали те расхожие сведения, которые нам сообщают киберсплетни, получившие название «фейков», поэтому склонны верить им как нашему априорному знанию, а не научным подсчетам и теоретизированиям. Таким образом, сам механизм функционирования нашего мозга, согласно представлениям современной когнитивной психологии, предопределяет его большую податливость воздействиям фейков, чем влиянию правдивой информации.

2. Эмоциональный уровень индивидуального сознания тоже легко становится «добычей» фейков. На эмоциональном уровне наиболее актуализирован сегодня в индивидуальном сознании страх – особый невротический страх как исторически обусловленный компонент сознания современного человека. В 50-е гг. XX века невротический страх усиливается «ядерным страхом». После изобретения оружия массового поражения растерянные и обезличенные люди начинают утрачивать веру в возможность воздействовать на мир и собственную судьбу. Позднее, после во-

йны в Персидском заливе в западных странах, да и во всем мире, распространяется синдром «ожидания катастрофы», причем он выглядит «чуть ли не празднеством по сравнению с черной хандрой, которая правит Францией» [17]. Страх как эффективный способ «отключения» здравого смысла и защитных механизмов сознания имеет благоприятную витальную среду в современном социуме. Человек, интериоризировавший страх, становится легко внушаемым по принципу «у страха глаза велики». Он легко верит в фейки алармистского характера, в разные вымышленные истории, генерирующие преувеличенный образ страха, хотя бы для того, чтобы нейтрализовать внутренний когнитивный диссонанс. Повышает уровень тревожности и сам характер социальных форумов, где как будто идет искреннее и доверительное общение между «френдами» (а не «брейнуошинг» официальной пропаганды), располагающее к тому, чтобы расслабиться, поделиться своими страхами, не сдерживая своего беспокойства, как в пьесе А.Н. Островского это делали странницы: «А то есть еще земля, где все люди с песьими головами»… Сейчас, правда, никто уже не верит, что есть страны, «где все люди с песьими головами», зато многие верят в фейк, что в Норвегии есть город, где нельзя умирать...

3. На уровне интенциональных состояний индивидуального сознания циркуляции фейков способствует экзистенциальное переживание современного человека в новом мире, который все больше развивается в направлении атеистической «смыслоутраты». Реализовать себя, оставить свой след на Земле, сказать так, чтобы все услышали – подобные мотивы побуждают многих участников соцсетей к постоянным высказываниям и оценкам в виртуальном пространстве. Вместо классического картезианского афоризма «Cogito ergo sum» «подключенный» человек современности мог бы сказать: «Loquor ergo sum». Участники интернет-форумов нередко высказываются о фильмах, которые пока не успели посмотреть или о товарах, которые курьер пока не успел им доставить[18], – просто потому, что факт инициации, участия в соцсетях для многих важнее с витальной и экзистенциальной точки зрения, чем достоверность мнения и оценки. Такие оценки «ради красного словца», точнее, симулякры оценок и становятся конструктами все новых и новых фейков, разрастающихся на благодатной почве уязвимости человеческого сознания.

В результате взаимодействия всех этих человеческих измерений в сети кон-фейкость превращается в конфекцию, поп-корн смешивается с поп-артом, мысли становятся пластиковыми, одноразовыми и дешевыми. «Все болтают, оскорбляют друг друга, возмущаются и забывают» [19].

Каким же образом можно противостоять этой свободе слова, вывернутой наизнанку?

Большинство исследователей, изучающих проблему информационного воздействия на сознание, считают, что построение системы информационной защиты является одной из наиболее трудных задач. По мысли Г.Г. Почепцова, арсенал информационного воздействия характеризуется достаточной долей гибкости, непредсказуемости, и по этой причине нелегко строить варианты обороны. С.П. Расторгуев считает, что для выявления информационной угрозы существующие способы защиты не подходят: «Действительно, система не может ни защититься оболочкой, ни убежать, ни уничтожить потенциального агрессора, ни даже самомодифицироваться» [20]. А.А. Волков констатирует принципиальную невозможность критического анализа реципиентом получаемой информации. Это связано с тем, что все материалы масс-медиа, объединенные системой ключевых слов и категорий с положительным и отрицательным значением, образуют своеобразный символический зонтик. «Поэтому сообщения массовой информации не могут быть критикованы получателем в пределах данной системы массовой информации» [21].

Тем не менее, по линии информационной защиты может быть гипотетически выстроена традиционная триада, включающая механизмы информационного реагирования на уровне государства, общества и личности.

На государственном уровне информационная защита опирается на юридический механизм, который оттачивается путем совершенствования законодательства. В этом плане два вышеупомянух федеральных закона («О внесении изменений в статью 15.3 Федерального закона “Об информации, информационных технологиях и о защите информации”» и «О внесении изменений в Кодекс Рф об административных правонарушениях»), а также находящийся в процессе утверждения закон о безопасной и устойчивой работе российского сегмента интернета, предполагающий целенаправленный контроль трафика рунета со стороны Роскомнадзора, ждут еще общественной оценки своей конституционности и эффективности.

Предварительно, однако, можно высказать несколько замечаний.

1. Удалению подлежит информация, не соответствующая действительности и распространяемая под видом достоверной информации. Однако никакой механизм верификации информации на предмет ее достоверности/недостоверности законодателями не предложен, расценен как излишний. Но информация, как известно, может иметь разную степень достоверности, и комбинации смыслов на этом семантическом поле бесчисленны: сущность информации может быть правдивой, но второстепенные детали могут содержать фактические неточности; или конкретные детали (указание места, времени) могут быть подчеркнуто достоверны, а изложение самого события некорректно; вся информация, изложенная в будущем времени, a priori является недостоверной и т.д. Законодатели предполагали, что степень достоверности информации будут определять Генеральный прокурор РФ и его заместители в рамках своих компетенций. Но ведь в компетенцию Генерального прокурора не входит работа по совместительству дегустатором в кафе, санитарным инспектором в клинике, завучем в школе, лингвоэкспертом в редакции, криминалистом в полиции и т.д. Предполагается, что решение Генерального прокурора может быть оспорено в судебном поряд-

ке, но ведь судебное решение тоже должно опираться на научно обоснованный механизм верификации подлинности новостей, а он не разработан – не сделано даже попытки его наметить, хотя бы в обобщенно-размытых формулировках, типичных для российского законодательства.

2. В соответствии с новым законом, подлежит удалению информация, которая «создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности...». Однако еще более общественно опасны случаи, когда удаление информации создает угрозу причинения вреда жизни и (или) здоровью..., как мы знаем из советского прошлого, когда нередко замалчивалась общественно значимая информация, способная посеять тревогу, например, уровень радиации после аварии на Чернобыльской АЭС: обнародованную недостоверную информацию можно, по крайней мере, перепроверить по разнообразным источникам и тем самым подключить методы борьбы с ней; нулевую информацию ни перепроверить, ни опровергнуть нельзя; между тем, с учетом отсутствия четко разработанных критериев верификации правды удаленный из информации факт может содержать в себе частицу правды (причем правды большой общественной значимости).

3. Есть опасность, что установление административных правонарушений за распространение недостоверных сведений на основе Федерального закона №27-ФЗ может повлечь за собой совершение уголовных преступлений, предусмотренных Уголовным кодексом РФ, в частности, статьей 292, квалифицирующей в качестве служебного подлога «внесение должностным лицом... в официальные документы заведомо ложных сведений».

Есть некоторые основания считать, что подобный казус произошел с первым применением Федерального закона №27-ФЗ «О внесении изменений в Кодекс РФ об административных правонарушениях»:

«В Архангельске составили административный протокол на активистку Елену Калинину, выступающую против строительства мусорного полигона. Поводом стала ее публикация в соцсети ВКонтакте с анонсом несогласованной протестной акции. В силовых структурах решили, что поскольку акция не разрешена, то не должна была состояться, а значит, информация о времени и месте ее проведения является фейковой». Утверждение, что несогласованные акции протеста не должны состояться на том основании, что они не согласованы, является заведомо ложным и опровергается многочисленными прецедентами российской социальной действительности; следовательно, внесение этого утверждения в официальные документы и применение на этом основании административных санкций может быть квалифицировано как служебный подлог.

На общественном уровне метастратегией информационной защиты было бы при всей своей исторической утопичности движение вспять от общества «постправды» к обществу, в котором правда в ее абсолютном, а не прагматичном измерении, является важнейшей общественной ценностью.

Как известно, в XX веке происходит смена когнитивных парадигм, в области теории истины намечается глубокий перелом, многие западные мыслители отказываются от понимания истины в абсолютном значении. В контексте интенсивных философских исканий XX века идеи релятивизма были близки, к примеру, Т. Адорно и М. Хоркхаймеру, предложившим теорию инструментальности разума и функциональности истины; К. Мангейму, признававшему социальную обусловленность любого мыслительного акта.

В теории массовых коммуникаций концепция релятивизация истины сформулирована еще в 20-е гг. XX века У. Липпманом: «Современная теория газетного дела в Америке состоит в том, что такая жалкая абстракция, как правда, и такая добродетель, как честность, должны быть принесены в жертву, когда кто-то думает, что этого требуют нужды цивилизации. Современная журналистика ... ставит правду на второе место после того, что в ее понимании составляет национальные интересы»[22]. Однако относительность истины в этом контексте сама имеет относительный характер, ибо при всем отрицании абсолютной правды автор признает существование возвышающейся над ней «метаправды»: «нужд цивилизации» и «национальных интересов».

Для теории истины не прошли бесследно и неоавангардистские эксперименты середины-конца XX века. Такие мэтры французского структурализма 60-х гг. XX века, как К. Леви-Стросс, Ж. Лакан, Р. Барт, М. Фуко исповедовали идею «множественной истины», превратив мировую историю в статическую картину неподвижных состояний, они релятивизировали идеи исторического движения, прогресса, истины. Постструктуралисты (Ж. Деррида, Ю. Кристева) предложили понимание истории как хаотического, «кишащего множеством диффузных функций процесса, лишенного минимального семантического ядра [23], то есть «множественную истину» структуралистов они заменили «множественностью без истины». Эти элитарные попытки редукции абсолютной истины к хаотической множественности смыслов не прошли бесследно для состояния массового сознания общества постмодерна, которое постепенно утрачивало восприимчивость к категориям истины-лжи в их классическом понимании.

Так закладывались идейные основы общества постправды, непременными атрибутами которого стали fake news. Тем не менее, в иерархии духовных ценностей современного человека поиск истины не утратил полностью своего смысла. В глубинах его души еще сохранилась та жажда раскрытия умом абсолютной истины, которая «открывается лишь вселенскому сознанию» (Н.А. Бердяев) и которая во многом предопределила пути русской философии и типологию национального сознания.

На уровне личности информационная защита имеет внешний и внутренний контуры.

Внешний контур информационной защиты личности образуется, в частности, деятельностью самих гигантов «мировой паутины», иногда противоречи-

вой: «Они могут множить заявления о решимости бороться с дезинформацией, но поскольку фейки сенсационны и заразительны, их запускают как механизм фуфло-бабло» [23]. Так, в 2017 г. гигант социальных сетей «Фейсбук» заявил об усилении борьбы с фейками путем надзора за подозрительным поведением в сети – повторными посланиями или закрытием счетов. Сюда же можно отнести лихорадочные попытки «Твиттера» идентифицировать сайты, связанные с российским правительством, которые якобы оказали влияние на результаты американских президентских выборов 2016 г. Некоммерческая организация «Mozilla Foundation» в 2017 г. запустила программу «Mozilla Information Trust Initiative» (MITI), предполагающую «полную мобилизацию усилий с целью сохранения общественного доверия и здорового интернета» и предусматривающую взаимодействие разнообразных форм: технологий, разработанных совместно с масс-медиа, образовательного ресурса в режиме реального времени, научно-исследовательских предложений и мер поддержки форумам и порталам» [23].

В этом же русле создаются инновационные технологии, компьютерные игры и программы оценки субъективного восприятия достоверности тех или иных событий и фейковости новостей. «Пользователю предлагается проверить свое умение отличать реальные новости от фейковых и получить звание эксперта в области выявления фальшивых новостей. Такова, например, PolitiTruth, некоммерческая игра, обучающая различать политический факт от вымысла. ... Проект завоевал Пулитцеровскую премию за сбор полезной статистики по общественным заблуждениям и поощрение игроков лучше различать источники информации» [23].

Внутренний контур информационной защиты личности предполагает меры индивидуальной психологической защиты, к которым прежде всего относится такая непревзойденная классика, как аналитическое чтение и критическое мышление.

Аналитическое чтение – это чтение глубокое, не ограничивающееся быстрым просмотром заглавий публикаций и «прикольных фоток»; это чтение вдумчивое, рефлектирующее; это чтение недоверчивое, критическое, возвращающееся вспять к уже прочитанному, забегающее вперед с целью подтверждения возникшей гипотезы, чтение, ищущее в информации противоречия; это чтение, воспринимающее не только явные, но и скрытые смыслы, подтекст и умеющее распознать технологии манипуляции сознанием, направленные на читателя; наконец, это чтение, способное в тоннах макулатуры выискать «золотые песчинки» метаинформации, сверхценной информации и слить их воедино для получения бурной химической реакции интеллекта – реакции озарения и прозрения в отношении смысла прочитанного.

Критическое мышление, по мысли французского психолога А. Мукейбера, складывается из трех умений: 1) умения задавать себе вопрос «почему», 2) умения культивировать в себе сомнение в отношении многообразных тем и сюжетов особенно тех, в которых мы особенно уверены; 3) умения «взвешивать» мнения, распределяя тот или иной процент доверия между разными точками зрения.

Литература

1. «И это не фейк. Меры против фейков ударят по сетевым террористам»//Российская газета. 2019. 19 марта; «Вступили в силу законы о фейковых новостях и оскорблении власти»//Российская газета. 2019. 23 марта.
2. Любимова Т.М. Язык лжи//Информационные войны. 2017. №4. С. 81-90.
3. Moles A. Sociodynamique de la culture. P. : Moutron , 1967. C.183-184.
4. Венедиктова Т.Д. Языки пепла//Новое литературное обозрение. 2015. №1(131). С. 371.
5. Вайзер Т. Языки лжи//Новое литературное обозрение. 2015. №1(131). С. 374-375.
6. Кара-Мурза С.Г. Манипуляция сознанием. М.: алгоритм. 2000. С. 82-83.
7. Delaye F. Fake news: le doute plane sur les géants de web// Bilan. 2017. 31 октября.
8. Paperjam. Business zu Lëtzebuerg. 2019. 18 января.
9. Иссерс О.С. Медиафейки: между правдой и мистификацией//Коммуникативные исследования. 2014. №2. С. 121.
10. Weissberg J.-L. Présences à distances. Déplacement virtuel et réseaux numériques: Pourquoi nous ne croyons plus la télévision. P. : Harmattan.
11. Sénécat A. Les mille et une ruses de l'industrie de la désinformation//Le Monde. 2017. 16 марта.
12. Серль Дж. Природа интенциональных состояний//Философия, логика, язык. М.: Прогресс, 108. С. 121.
13. Notre cerveau face au FAFE NEWS – Albert Moukheiber parle avec/https:www.youtube.com/watch ?v=esf+b-2f=4i. 14 апреля 2019.
14. Зимбардо Ф., Ляйппе М. Социальное влияние. Спб: Питер, 2000. С. 172.
15. Сегела Ж. Национальные особенности охоты за голосами. М.: Вагриус, 1999. С. 211.
16. Schauder T. Toutes les paroles se valent-elles?//Le Monde Campus. 2019. 12 марта.
17. Расторгуев С.П. Информационная война. С. 217. М.: Радио и связь, 1999. С. 217.
18. Волков А.А. Курс русской риторики. М.: Изд-во храма св. муч. Татианы, 2001. С. 59.
19. Lippman W. Liberty and the News. New York, 1920. С. 8-9.
20. Деррида Ж. Фрейд и сцена письма// Французская семиотика: от структурализма к постструктурализму. М.: Прогресс, 2000. С. 340.
21. Delaye F. Fake news: le doute plane sur les géants de Web//Bilan. 2017. 31 октября.
22. Mozilla amplifie ses efforts contre les "fake news"//Bilan. 2017. 9 августа.
23.Забарин А.В. Инновационные технологии создания фейков: новые вызовы информационной безопасности России//Информационные войны. 2018. №4. С. 65.

Материал поступил в редакцию 17.09.2019 г.

III. ИСТОРИЯ КАК ОБЪЕКТ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

УДК 32.019.51

© Зайцев И.О.

© Zaytsev I.

ИНФОРМАЦИОННАЯ КАМПАНИЯ ПРОТИВ НЕСИСТЕМНОЙ ОППОЗИЦИИ В 2011 – 2012 ГГ.

INFORMATION CAMPAIGN AGAINST THE NON-SYSTEMIC OPPOSITION IN 2011 - 2012

Аннотация. *Статья посвящена информационной кампании, проведенной в 2011 – 2012 гг. против активизировавшей протестную деятельность несистемной оппозиции. Рассматриваются основные этапы информационной кампании, использовавшиеся технологии, идейные установки, транслировавшиеся в информационном поле. В исследовании вводятся и разъясняются авторские термины «активная фаза информационной кампании», «инерционная фаза информационной кампании», «гибридная информационная кампания», «реактивная информационная кампания». По итогам исследования делается вывод о неоднородности кампании против несистемной оппозиции, включении в нее новых элементов и достижений, в конечном итоге предполагаемых целей.*

Abstract. *The article is devoted to the informational campaign conducted in 2011 – 2012 against the non-systemic opposition that has activated the protest activity. The main stages of the informational campaign, the technologies used, the ideological installations that were broadcast in the information field are considered. The study introduces and explains the author's terms «active phase of the informational campaign», «inertial phase of the informational campaign», «hybrid informational campaign», «reactive informational campaign». According to the results of the study, a conclusion is drawn about the heterogeneity of the campaign against the non-systemic opposition, the inclusion of new elements in it, and the achievement, ultimately, of the alleged goals.*

Ключевые слова. *Информационная кампания, активная фаза, информационно-политические технологии, коммуникации, пропаганда.*

Key words. *Informational campaign, active phase, information-political technologies, communications, propaganda.*

Массовые выступления внесистемной оппозиции, начавшиеся сразу после выборов в Государственную Думу VI созыва в декабре 2011 г., стали заметным явлением на отечественной политической сцене. Оппозиция представляла собой конгломерат партий, движений и граждан разных идеологических ориентаций, недовольных результатами выборов. Протестные митинги охватили большое число российских городов, крупнейшие из них прошли в Москве. Несмотря на то, что митинги в целом носили мирный характер, 6 мая 2012 г. в Москве, на Болотной площади, произошли столкновения демонстрантов с полицией, что впоследствии привело к возбуждению ряда уголовных дел. Российской власти, против которой было направлено большинство лозунгов оппозиции, пришлось оперативно вырабатывать методы противодействия, в том числе в информационной сфере. В результате была проведена массированная информационная кампания, активная фаза которой приходилась на 2011 – 2012 гг.

При исследовании информационных кампаний могут возникать трудности с определением их временных рамок. После завершения кампании свойственные ей сообщения могут с меньшей интенсивностью продолжать появляться в информационном поле. Поэтому мы вводим понятия активной фазы и инерционной фазы информационной кампании [12]. Активная фаза представляет собой координированное информационное воздействие посредством максимального количества доступных каналов. Инерционная фаза вступает в силу после завершения активной и представляет собой отдельные сообщения по ряду каналов, характерные для активной фазы, но не создающие массированного информационного потока. После завершения активной фазы кампании продолжение транслирования свойственных ей сообщений способствует привлечению внимания к политическим акторам и информационным ресурсам, так как поднимавшиеся ранее темы вызывали всеобщий ажиотаж.

В отношении первых митингов оппозиции, состоявшихся 4, 5 и 6 декабря 2011 г. в Москве, была выбрана тактика замалчивания. Игнорируя данный информационный повод, центральные каналы телевидения освещали митинги сторонников «Единой России», проходившие одновременно с оппозиционными [22]. С 10 декабря протесты увеличились территориально и количественно, охватив многие города России, а также зарубежья. Крупнейшие митинги прошли 10 и 24 декабря 2011 г. в столице на Болотной площади и проспекте Сахарова. Протесты стали фактором, замолчать который в условиях современной информационной среды было невозможно, поэтому тележурналисты начали выборочно транслировать информацию. В частности, ряд сюжетов и телепрограмм, подробно рассказывавших о протестах, были первона-

Зайцев Игорь Олегович *– соискатель, исторический факультет, МГУ им. Ломоносова, e-mail: ingvanir@gmail.com.*

Zaytsev Igor *– applicant, faculty of history, Lomonosov Moscow State University, e-mail: ingvanir@gmail.com.*

чально сняты с эфира канала НТВ [37], однако в начале 2012 г. лидеры оппозиции все же появились на этом канале и участвовали в дискуссии с оппонентами в рамках передачи «НТВшники» [11, 38].

До февраля 2012 г. жесткую критическую позицию по отношению к протестам в печати занимали только небольшие проправительственные издания. С февраля была предпринята попытка массированного информационного воздействия на граждан посредством печати, что выразилось в издании газеты «Не дай Бог!». Газета распространялась бесплатно в виде вложений в «Аргументы и факты»[1] и «Комсомольскую правду»[2] и раздачи на улицах. Вышло 5 номеров газеты, тираж каждого составил 5490000 экземпляров, что делает «Не дай Бог!» на момент выхода самым массовым печатным изданием страны. Название газеты восходило к антикоммунистическому изданию периода президентских выборов 1996 г., направленному против Г. Зюганова [24].

Основную массу статей, содержавшихся в номерах газеты, можно разделить на несколько групп. В первую входят статьи, направленные на возбуждение страха перед результатами революции и приходом к власти лидеров протестов, они построены как на исторических примерах [34, 6], так и на конструировании гипотетического сценария победы оппозиции [30, 31, 5]. Возбуждение страха достигалось муссированием двух сюжетов: вероятного резкого ухудшения жизни простых граждан и эскалации насилия вследствие роста бандитизма и активизации политических радикалов. Другая группа материалов внедряла ощущение «осажденной крепости», связывая протестную активность с прямым влиянием США и других стран Запада в революционных событиях прошлого и настоящего [33, 15, 21, 14]. Третья группа текстов содержала противопоставление участников протеста гражданам, не посещающим оппозиционные митинги, и обращалась к разделению на «мы и они» [19, 13]. К четвертой группе относятся высказывания известных личностей, близких к оппозиции [4, 18, 20, 16], но критиковавших ее отдельные лозунги или действия, что было призвано делегитимировать протест. Последнюю группу составили статьи, позитивно оценивающие деятельность В. Путина, а также утверждавшие необходимость взаимодействия между избранным президентом и оппозицией [23, 9, 39] и пытавшиеся, таким образом, «абсорбировать» оппозиционный потенциал.

Главной идейной установкой, содержащейся в материалах газеты, было неприятие революции, выраженное с консервативных позиций. Консервативные идеалы в целом превалировали в выпусках издания, кроме последнего номера, который также содержал мнения людей с разными взглядами, что можно трактовать, как стремление представить идейно-политический консенсус по поводу состоявшихся президентских выборов. Из пропагандистских приемов, используемых в «Не дай Бог!», основным был присоединение аудитории к чувству страха. Использование в газете слов лидеров и сторонников оппозиции было направлено на привлечение аудитории из числа поддерживающих протесты граждан. Протестные настроения обладали функцией барьера [10], не позволяющего оппозиционерам воспринимать доводы направленной против них пропаганды, а данные материалы помогали преодолеть барьер. Все номера «Не дай Бог!» содержали статьи, возбуждающие в реципиентах чувство страха перед революционными изменениями и их последствиями. Страх является одним из самых простых и при этом сильных чувств, поэтому нагнетание страха используется как инструмент убеждения [3], в данном случае убеждения читателей в недопустимости победы оппозиции.

С марта 2012 г. в информационную кампанию активно включилось российское телевидение. Из направленных против оппозиции видеоматериалов наибольший общественный резонанс [32, 29] вызвали показанные по центральным каналам документальные фильмы «Анатомия протеста» [1] и «Анатомия протеста 2» [2]. Задачей обоих фильмов была максимальная дискредитация оппозиции. Она обвинялась в отсутствии позитивной программы, в провокации на митинге в поддержку В. Путина в Лужниках, в привлечении на свои акции массовки за деньги, манипуляциях с информацией в Интернете и др. Главной идеей становилась координация действий оппозиции со стороны американских политиков и дипломатов – прием, вызывавший отклик у массы избирателей в условиях подпитывавшихся ранее антиамериканских и антизападных настроений. Во второй части фильма внесистемная оппозиции в лице одного из ее лидеров, С. Удальцова, увязывалась с «экспертом» в организации «цветных революций» Г. Таргамадзе, эмигрировавшими в Великобританию российскими олигархами, криминалитетом, американскими советниками и пр. Все это вместе служило задаче массированной негативизации имиджа оппозиционеров.

Авторы первого фильма использовали прием под названием «переводом стрелок»: обвинения в нечестности были перенесены с власти на оппозицию [25]. Учитывая, что честность (выборов и политической деятельности в целом) была фактически главной декларируемой идеей оппозиции, обвинения ее самой в фальсификациях и манипуляциях имели большое стратегическое значение. Во втором фильме выводы, полученные из компромата на одного из лидеров оппозиции, экстраполировались на всех ее знаковых фигур, причем эксклюзивность снятых скрытой камерой кадров служила хорошим способом привлечения внимания к фильму.

Параллельно с информационно-пропагандисткой кампанией, направленной против внесистемной оппозиции, с весны 2012 г. стала разворачиваться информационная кампания вокруг панк-группы оппозиционной направленности «Pussy Riot», которая также оказывала воздействие на информационное поле в

[1] С №7 (1632) от 15-21 февраля 2012 г. по №11 (1636) от 14-20 марта 2012 г.
[2] С №7-т (25836-т) от 16-23 февраля 2012 г. по №11-т (25851-т) от 15-22 марта 2012 г.

рамках борьбы с оппозицией. «Акционистские» действия участниц группы у алтаря храма Христа Спасителя стали причиной возбуждения уголовного дела, судебного процесса над ними и вынесения приговора, вызвавшего большой международный резонанс [7, 17, 36]. Вокруг данного повода был сформирован мощный информационный поток, и насыщенность медийного поля сообщениями, посвященными делу «Pussy Riot», заставляла реципиентов так или иначе реагировать на него, принимая ту или иную точку зрения. Внушительная часть коммуникаций в мире была направлена на поддержку участниц группы, в России также имелись их сторонники, начиная с тех, кто полностью одобрял их поступок, и заканчивая теми, кто счел приговор излишне строгим. В этих условиях российская власть стала транслировать собственный коммуникационный поток, создающий негативный образ панк-группы в общественном сознании.

Наиболее яркими материалами, использованными в этой кампании, являются авторские документальные фильмы А. Мамонтова, показанные в рамках передачи «Специальный корреспондент» по каналу «Россия-1» вместе с последующей дискуссией между гостями в студии [26-28]. Акция «Pussy Riot» связывалась с деятельностью жившего в Великобритании олигарха Б. Березовского и ставилась в один ряд с митингами внесистемной оппозиции. Поддержка, оказывавшаяся участницам группы, интерпретировалась как целенаправленная акция, спланированная на Западе. Упоминались связь группы с окружением С. Удальцова, контакты этого окружения с Г. Таргамадзе. В целом «образ врага» конструировался практически по тем же лекалам, что и в предыдущем случае, и дополнялся мотивом нападок на церковь со стороны абстрактной демонизированной общности, состоящей из сторонников панк-группы, оппозиционеров и западных акторов.

Тема «Pussy Riot» поднималась в центральных СМИ России и ранее апреля 2012 г., когда вышел первый фильм Мамонтова, становилась главной темой в различных ток-шоу, где спорили сторонники и противники обвиняемых, но одностороннего целенаправленного пропагандистского воздействия еще не применялось. Существует версия, что кампания вокруг акции в храме проводилась с целью отвлечь общественное внимание от идущих в стране протестов [35]. Однако, на наш взгляд, ситуация обстояла несколько иначе. В первую очередь, раскручивание данной кампании было выгодным под углом зрения более важной задачи – дискредитации политической оппозиции. Кампания против панк-группы способствовала как нарастанию негативного представления о протестах среди электората, так и расколу в оппозиционных рядах. Эклектичная по своей структуре внесистемная оппозиция включала в себя тех, кто поддерживал либо осуждал акционисток. Необходимость в условиях развертывавшейся кампании озвучивать свое мнение стимулировала возникновение разногласий среди оппозиционеров. Согласно социологическим данным ФОМ, опубликованным в августе 2012 г., большинство респондентов считали вынесенный приговор справедливым (53%) и отрицательно относились к акции в храме (66%) [8]. В этих условиях поддержка панк-группы частью протестующих снижала рейтинги оппозиции. С другой стороны, вторая и третья части фильма вышли в эфир после оглашения резонансного приговора участницам группы и на фоне проходящей в западных странах медийной кампании в поддержку осужденных. В этих фильмах прослеживается желание российских акторов противопоставить собственную точку зрения защитникам группы в России и мире.

Таким образом, кампания против панк-группы, с одной стороны, отвечала на масштабный инфопоток в России и зарубежных СМИ, направленный на поддержку участниц коллектива, а с другой – связывала деятельность группы с внесистемной оппозицией и западными акторами, что способствовало дальнейшей дискредитации протестной активности. Для обозначения кампании вокруг «Пусси Райот» мы вводим термин «гибридная информационная кампания». Гибридная кампания входит составной частью в две или более информационные кампании, поводом для начала такой кампании может послужить одно событие (например, громкий информационный повод), но транслируемые в ее рамках коммуникационные потоки используются в нескольких кампаниях, в том числе не связанных с причиной начала основной кампании напрямую. В описываемом случае поводом к возникновению кампании была акция «Pussy Riot», но коммуникации этой кампании стали составной частью активной фазы информационной кампании против оппозиции.

В конце 2012 – начале 2013 гг. протесты начали спадать, в информационном поле продолжали появляться отдельные сообщения, направленные против оппозиции, но активная фаза кампании была закончена. Оценить прошедшую кампанию можно через анализ ее составных частей: идеологического контента, психологического воздействия и наработок из сферы предшествующего пропагандистского опыта.

1. Идеологическая составляющая выражалась в пропаганде комплекса консервативных идей, включая недопустимость революционных изменений, апологию сильной власти и защиту суверенитета страны от внешних влияний.

2. Психологическое воздействие преимущественно сводилось к возбуждению чувства страха перед протестующими, выстраиванию схемы «мы и они»; формированию «образа врага». Идеологическое и психологическое воздействие тесно переплетались и подпитывали друг друга.

3. Наиболее заметным и буквальным использованием исторического опыта стало распространение высокотиражной бесплатной газеты, унаследовавшей от прототипа в том числе и название.

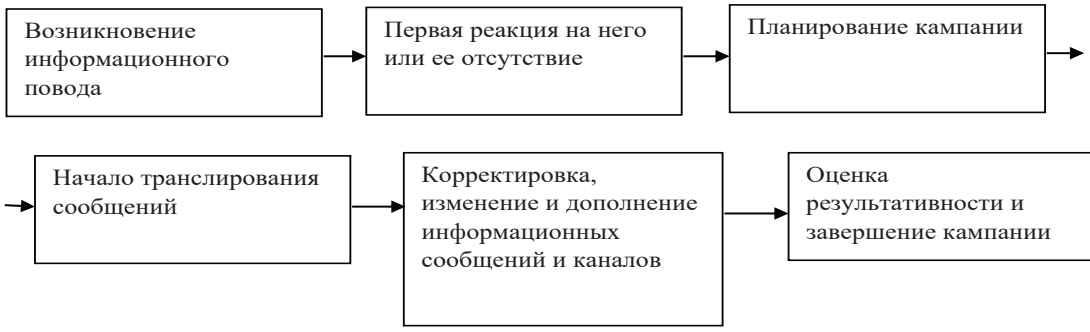
В ходе информационной кампании применялись по большей части технологии убеждения и использования образов, насаждавшие заданное восприятие деятельности внесистемной оппозиции. Зеркальный перенос обвинений с одной стороны на другую, экстраполяция негативных последствий деятельности оппозиции в будущее, задействование религиозный фрей-

мов, противопоставление основной массы граждан и оппозиции («мы и они»), педалирование ощущения внешней опасности, демонизация оппозиционных деятелей – все это было активно применено для делегитимации протестных действий.

Исследование информационной кампании против оппозиции позволяет говорить о том, что она относится к особой модели, называемой нами реактивной. Реактивная модель информационной кампании представляет собой целенаправленное информационное воздействие, применяющееся после возникновения громкого информационного повода и в качестве реакции на него. Фаза планирования кампании наступает после возникновения инфоповода. Необходимость быстрой реакции на повод и недостаток времени для планирования могут приводить к тому, что применяемая в рамках кампании стратегия корректируется и меняется по ходу кампании. При использовании реактивной модели кампании отпадает технология «постепенного ввода» отдельных сообщений в информационное поле для подготовки общественного мнения. Оно уже реагирует на инфоповод, и целью кампании является быстрое изменение представлений реципиентов с учетом целей коммуникатора. Во время проведения кампании транслируемые сообщения могут оперативно изменяться, кампания может включать в себя новые элементы и каналы коммуникации по мере получения новой информации (см. рисунок).

При применении модели к рассматриваемой кампании мы получаем следующее: возникновение протестной активности – период замалчивания или предвзятого информирования – быстрое планирование кампании – начало систематической трансляции сообщений посредством печати и телевидения – корректировка и дополнение, включая кампанию против «Pussy Riot» – спад протестной активности и завершение кампании.

Типологически кампания против несистемной оппозиции имела внутриполитический характер, выполнялась на федеральном уровне, по темпам проведения ее можно отнести к кампаниям нарастающей интенсивности. Поскольку протестная активность в конечном итоге стала затухать, предполагаемая цель кампании была выполнена. Вероятно, в достижении результата сыграли роль и примененные властью информационно-политические технологии, и другие причины: эклектичность оппозиции, неудачный выбор озвучиваемой повестки, непродуманный план действий. Тем не менее, критерием оценки информационной кампании служит ее эффективность, поэтому рассматриваемую кампанию можно назвать успешной.



Элементы транслируемых сообщений

Литература

1. Анатомия протеста. URL: http://www.ntv.ru/video/peredacha/296996/ (Дата обращения: 04.10.2019).

2. Анатомия протеста-2. URL: http://www.ntv.ru/video/354142/ (Дата обращения: 04.10.2019).

3. Аронсон Э., Пратканис Э. Эпоха пропаганды: Механизмы убеждения повседневное использование и злоупотребление. – СПб.: Прайм-Еврознак, 2002. – 384 с.

4. Белинова В. Виктор Ерофеев: «Это не гражданская война – это война ценностей» // Не дай Бог! – М., 2012. – 15–21 февраля, №1. – С. 6.

5. Глинкин И. Ваш жилищный вопрос не будет решен никогда // Не дай Бог! – М., 2012. – 7–13 марта, №4. – С. 7.

6. Глинкин И. Сбережения опять сгорят // Не дай Бог! – М., 2012. – 15–21 февраля, №1. – С. 7.

7. Дело Pussy Riot вызвало международный резонанс. URL: http://www.ng.ru/politics/2012-07-23/1_pussy.html (Дата обращения: 04.10.2019).

8. Дело Pussy Riot: общественный резонанс. URL: http://fom.ru/obshchestvo/10606 (Дата обращения: 04.10.2019).

9. Дугин А. История ловит Путина на слове… // Не дай Бог! – М., 2012. – 14–21 марта, №5. – С. 4.

10. Евгеньева Т.В. Технологии социальных манипуляций и методы противодействия им. – СПб.: Питер, 2007. – 112 с.

11. Если не Путин, то кто? URL: https://www.ntv.ru/video/1734519/ (Дата обращения: 04.10.2019).

12. Зайцев И.О. Российская информационная кампания в период вооруженного противостояния на востоке Украины в 2014 – 2015 гг. // Россия и современный мир. – 2018. – №3. – С. 213–222.

13. Клименко Г. «Бывшее офицерье на митинги не ходит» // Не дай Бог! – М., 2012. – 29 февраля – 6 марта, №3. – С. 2.

14. Константинов В. Андрей Фурсов. Как не превратить март 2012-го в февраль 1917-го // Не дай Бог! – М., 2012. – 29 февраля – 6 марта, №3. – С. 4–5.

15. Крашенинникова В. Подрыв власти: мягкие технологии // Не дай Бог! – М., 2012. – 22–28 февраля, №2. – С. 5.

16. Левич Б. Лидеры оппозиции призывают своих сторонников не поддаваться на провокации // Не дай Бог! – М., 2012. – 7–13 марта, №4. – С. 3.

17. Ли У. О Pussy Riot и Путине говорили 86% мировых средств массовой информации. URL: https://www.golos-

ameriki.ru/a/media-on-pussy-riot/1490739.html (Дата обращения: 04.10.2019).
18. Мамонтов В. Алексей Венедиктов: Что меня коробит в лозунге «Путин, уходи!» // Не дай Бог! – М., 2012. – 22–28 февраля, №2. – С. 6.
19. Мамонтов В. Болотная – Поклонная: куда двинется страна? // Не дай Бог! – М., 2012. – 15–21 февраля, №1. – С. 1.
20. Мамонтов В. Григорий Явлинский: «Мы должны избежать насилия и кровопролития» // Не дай Бог! – М., 2012. – 7–13 марта, №4. – С. 1.
21. Митрополит Агафангел. Оранжевые метят в сердце Святой Руси // Не дай Бог! – М., 2012. – 22–28 февраля, №2. – С. 5.
22. Михайлов О. Протесты оппозиции в России: интернет кипит, ТВ молчит. URL: http://www.bbc.com/russian/russia/2011/12/111207_russia_protests_media_coverage.shtml (Дата обращения: 04.10.2019).
23. Осин А. Поэтому я голосую «за» // Не дай Бог! – М., 2012. – 7–13 марта, №4. – С. 6.
24. От редакции // Не дай Бог! – М., 2012. – 15–21 февраля, №1. – С. 1.
25. Политические коммуникации: Учеб. пособие для студентов вузов. Под ред. А.И. Соловьева. – М.: Аспект Пресс, 2004. – 332 с.
26. Провокаторы. URL: https://www.youtube.com/watch?v=aeT0dZbGkzc (Дата обращения: 04.10.2019).
27. Провокаторы-2. URL: https://www.youtube.com/watch?v=z0oHHEtcMdM (Дата обращения: 04.10.2019).
28. Провокаторы-3. URL: https://www.youtube.com/watch?v=dnTjEpSBMdI (Дата обращения: 04.10.2019).
29. Реакция на фильм НТВ «Анатомия протеста-2». URL: https://ria.ru/trend/Anatomy_of_protest_06102012/ (Дата обращения: 04.10.2019).
30. Сергеева М. «Что я скажу детям, если мы снова развалим страну?» // Не дай Бог! – М., 2012. – 22–28 февраля, №2. – С. 1–2.
31. Сидоренко О. Убийства, грабежи, разбои // Не дай Бог! – М., 2012. – 22–28 февраля, №2. – С. 7.
32. Скандал вокруг фильма «Анатомия протеста» на телеканале НТВ. URL: https://ria.ru/trend/ntv_scandal_17032012/ (Дата обращения: 04.10.2019).
33. Снегирев Ю. «Предложили стать министром. Отказался – дорого, 50 000 долларов» // Не дай Бог! – М., 2012. – 22–28 февраля, №2. – С. 4.
34. Соколовская Я. Как Украина меняла голубое сало на оранжевое мыло // Не дай Бог! – М., 2012. – 15–21 февраля, №1. – С. 4–5.
35. Соловей В.Д. Абсолютное оружие. Основы психологической войны и медиаманипулирования. – М.: Эксмо, 2015. – 320 с.
36. Сущность путинской России. Приговор Pussy Riot стал центральной темой в зарубежных СМИ. URL: https://lenta.ru/articles/2012/08/19/pussymedia/ (Дата обращения: 04.10.2019).
37. Умолчать о главном. Какие сюжеты НТВ снял с эфира в 2011 году. URL: http://lenta.ru/articles/2011/12/26/ntvfinal/ (Дата обращения: 04.10.2019).
38.Февральская эволюция? URL: https://www.ntv.ru/video/1734520/ (Дата обращения: 04.10.2019).
39.Шмаров А. А страна ждет согласия // Не дай Бог! – М., 2012. – 14–21 марта, №5. – С. 5.

Материал поступил в редакцию 07.10.2019 г.

IV. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 338.24

© Цыганов В.В., Корепанов В.О.
© Tsyganov V., Korepanov V.

МОДЕЛИ, МЕТОДЫ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ АКТИВНЫХ СИСТЕМ ПРИ ПРЕДЕЛАХ РОСТА

MODELS, METHODS AND INFORMATION TECHNOLOGY SECURITY MANAGEMENT OF ACTIVE SYSTEMS WITH GROWTH LIMITS

Аннотация. *Исследуются проблемы управления безопасностью общества, состоящего из целенаправленно действующих (активных) элементов. Рассмотрены нейропсихологические модели активного элемента, управляемого желаниями удовольствий и страхами наказаний. Введено понятие смысла его жизни, связанное с надеждой на положительные эмоции в будущем. Предполагается, что безопасность общества обеспечивается наличием смысла жизни каждого из его членов. Рассмотрен активный элемент, действующий в благоприятной среде – Прогрессист, управляемый желаниями. Доказано, что для безопасности общества, состоящего из Прогрессистов, необходимо и достаточно последовательности стимулов, способствующих выполнению желаний каждого члена сообщества. Показано, что противоречие между ростом потребления и ограниченностью ресурсов биосферы приводит к социально-политической нестабильности общества потребления. Другой тип активного элемента - Фобик действует в неблагоприятной среде, генерирующей раздражения. Поэтому Фобиком управляют страхи. Определены условия, при которых регулярные раздражения (наказания) обеспечивает смысл жизни Фобика. При этом общество Фобиков безопасно. На основе полученных теоретических результатов рассмотрены информационные технологии социальной безопасности. Проанализировано влияние массовых фобий, в частности, фобии ядерной войны. Предложены пути разрешения основного противоречия между ростом потребления и ограниченностью ресурсов биосферы.*

Abstract. *The problems of security management of a society consisting of purposefully acting (active) elements are investigated. The neuropsychological models of the active element controlled by the desires of pleasure and the fear of punishment are considered. Introduced the concept of the meaning of his life, associated with the hope of positive emotions in the future. It is assumed that the safety of society is ensured by the presence of the meaning of life of each of its members. Considered the active element acting in a favorable environment - Progressist, driven by desires. It is proved that for the safety of a society consisting of Progressists, it is necessary and sufficient sequence of incentives that contribute to the wishes of each member of the community. It is shown that the contradiction between the growth of consumption and the limited resources of the biosphere leads to the socio-political instability of the consumer society. Another type of active element - Phobic acts in an unfavorable environment that generates irritation. Therefore, Phobic is controlled by fears. The conditions under which regular irritation (punishment) provides the meaning of Phobik's life are defined. At the same time, the Phobic society is safe. On the basis of the obtained theoretical results, information technologies of social security are considered. The influence of mass phobias, in particular, phobias of nuclear war, is analyzed. The ways of resolving the main contradiction between the growth of consumption and limited resources of the biosphere are proposed.*

Ключевые слова. *Пределы роста, социальная безопасность, желание, страх, стимул, поощрение, наказание, фобия.*

Key words. *The limits of growth, social security, desire, fear, incentive, encouragement, punishment, phobia.*

1. Введение

В демократическом обществе социальная стабильность традиционно поддерживается обратной связью членов общества с политиками. Эта обратная связь реализуется путем голосования на выборах, формирования рейтингов политиков и др. Однако пределы глобального роста, возникающие вследствие ограниченности природных ресурсов и потенциала самовосстановления окружающей среды [1], ведут к стагнации и социальной нестабильности [2]. Растущее протестное сознание выражается в голосовании против политики правящих элит в странах Запада. Соответствующие современные нелиберальные и квазидемократические тенденции были предсказаны ещё Ф. Закарией [3]. Они приводят к появлению токсичных лидеров и коррумпированных политиков [4], лидеров без этики [5] и олигархии [6], угрожающих социально-политической стабильности. В связи с этим необходимо создавать информационные технологии общественной безопасности в условиях пределов роста. Для этого, прежде всего, необходима соответствующая модель члена общества. До сих пор широко использовались социальные и рациональные модели человека, восходящие к Г. Саймону [7]. Также известны модели человеческого поведения, основанные на психологии и теории игр. Они широко признаны в научном сообществе, в том

Цыганов Владимир Викторович *– доктор технических наук, профессор, главный научный сотрудник, ИПУ РАН;*
Корепанов Всеволод Олегович *– кандидат технических наук, старший научный сотрудник, ИПУ РАН, тел.+7(495)334-90-51, E-mail: vkorepanov@ipu.ru.*

Tsyganov Vladimir *– doctor of technical sciences, professor, professor, chief researcher, IPU RAS;*
Korepanov Vsevolod *– candidate of technical sciences, senior researcher, IPU RAS, tel. + 7 (495) 334-90-51,E-mail: vkorepanov@ipu.ru.*

числе отмечены Нобелевскими премиями. Примеры – теория психоанализа [8] и теория перспектив [9].

С развитием нейронаук появилась возможность строить более адекватные модели человека, учитывающие не только его рациональность, но и чувственность, эмоциональность. В основе этих моделей лежат результаты современных нейрофизиологических исследований связи поведения людей с их гормональными характеристиками [10]. На их основе была разработана модель дальновидного человека, управляемого собственными желаниями [11]. По сути, это модель эмоционально-рационального человека, использующего имеющиеся возможности для достижения текущих и будущих целей. Например, на основе этой модели разрабатывались высокие гуманитарные технологии в политической системе общества [12]. Эта же модель использовалась в социологических исследованиях общественной безопасности [13]. С её помощью были установлены связи пределов роста, стагнации, креативности и международной стабильности [14]. В этой статье мы сосредоточимся на проблеме разработки моделей, методов и информационных технологий обеспечения социально-экономической стабильности и общественной безопасности с учетом не только желаний, но и страхов членов общества.

2. Модель и методы обеспечения социальной безопасности на основе желаний

2.1. *Ощущения, эмоции и смысл жизни Прогрессиста*

Элемент социальной системы, имеющий собственные цели и возможности для их достижения, называется активным [13]. Рассмотрим активный элемент (АЭ), на которого оказывается позитивное внешнее воздействие (поощрение) s_t, возникающее в момент o

$$s_t = \begin{cases} s > 0, & \text{если } o \le t \le o + e; \\ 0, & \text{если } t < o \text{ или } t > o + e, \end{cases} \qquad (1)$$

где t – время. Такой АЭ называется Прогрессистом. Сплошная линия на рис. 1,*a* показывает первичную реакцию (ощущение) Прогрессиста Y_t при поощрении s_t Такая реакция типична, например, для эмпирических исследований кожно-гальванической реакции, где Y_t – кожно-симпатический вызванный потенциал, измеряемый в микровольтах, t – время в миллисекундах [11]. Подобный вид имеют нейропсихологические реакции и в других масштабах (например, реакции на уровне нейронов).

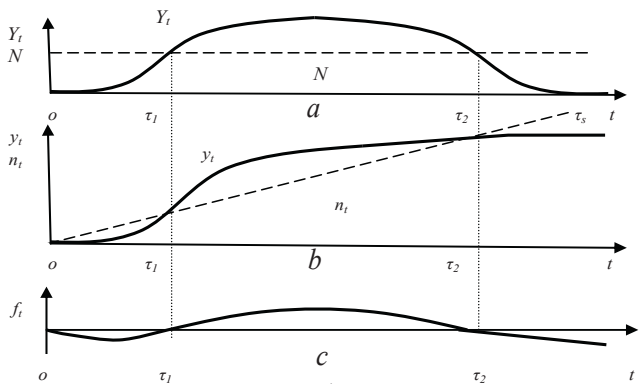


Рис. 1. Реакция Прогрессиста на поощрение s_t: *a* – первичная; *b* – интегральная; *c* – эмоции Прогрессиста f_t

З. Фрейд показал, что для психического здоровья человеку требуются некоторый минимальный уровень ощущений [8]. На рис. 1,*a* этот уровень показан пунктирной линией. Это так называемая нейрофизиологическая норма N. Сплошная линия на рис. 1,*b* показывает вторичную интегральную реакцию

$$y_t = \int_0^t Y_\tau d\tau,$$

объединяющую информацию о прошлых и текущих первичных реакциях. Соответствующее нормативное значение y_t – интегральная психологическая норма

$$n_t = \int_o^t N d\tau = (t - o)N$$

показана пунктирной линией на рис. 1,*b*.

Реакция Прогрессиста на внешние раздражители выражается в эмоциях

$$f_t = F(n_t, y_t) = \begin{cases} F(n_t, y_t) \ge 0, & if \quad y_t \ge n_t; \\ F(n_t, y_t) < 0, & if \quad y_y < n_t, \end{cases} \qquad (2)$$

где $F(n_t, y_t)$ – эмоциональная функция [11]. Зависимость эмоций (2) при поощрении (1) показана на рис. 1,*c*.

З. Фрейд связывал инстинкт жизни с надеждой на получение положительных эмоций в будущем [8]. Формализуем понятие смысла жизни, связанной с такой надеждой.

Определение 1. Будем говорить, что жизнь АЭ имеет смысл, если для любого момента времени t существует момент v, $v \ge t$, такой что эмоции АЭ положительны: $F(n_v, y_v) > 0$. Формально, это можно записать в виде

$$\forall t \ \exists v \text{ такое, что } v \ge t, \text{ и } F(n_v, y_v) > 0. \qquad (3)$$

Если условие (3) не выполняется, будем говорить, что жизнь АЭ не имеет смысла.

Будем говорить, что положительные ощущения Y_t, показанные на рис.1, формируют благоприятную ситуацию для Прогрессиста.

Утверждение 1. Жизнь Прогрессиста в благоприятной ситуации не имеет смысла.

Доказательство. Первичная и интегральная реакции Прогрессиста на поощрение s_t, а также его эмоции f_t показаны на рис. 1. Как видно на рис. 1,*b* и рис. 1,*c* $y_t < n_t$ и $F(n_t, y_t) < 0$ при достаточно больших t. Таким образом, не существует v такого, что $v \ge t$ и $F(n_v, y_v) > 0$. Следовательно, условие (3) не выполняется. Отсюда, используя определение 1 (при условии, что АЭ является Прогрессистом), получаем, что жизнь Прогрессиста не имеет смысла, что и требовалось доказать.

По сути, бессмысленность жизни Прогрессиста обусловлена отсутствием внешних воздействий, ведущих к новым удовольствиям. Действительно, из рис.1,*c* видно, что положительные эмоции, связанные с удовлетворением желания Прогрессиста, в конце концов, проходят. «Все проходит», – говорил царь Соломон. Поэтому Прогрессисту требуются регулярные внешние воздействия – поощрения, за которым следуют новые положительные эмоции.

2.2. *Лестница желаний и безопасность общества Прогрессистов*

Утверждение 2 формально отражает проблему застоя − противоречие между стремлением к удовольствию в благоприятной ситуации и необходимостью уйти от неё, чтобы предотвратить потерю смысла жизни. По сути, эта проблема связана с отсутствием новых ощущений при чрезмерно спокойной жизни. Субъективно Прогрессист рассматривает его как регресс, побуждающий к протесту. Его разочарование и агрессия могут обращаться на других людей, общество и существующий порядок.

В связи с этим будем исходить из того, что безопасность общества гарантируется наличием смысла жизни для каждого его члена. Тогда из вышесказанного следует, что общество, состоящее из Прогрессистов, при благоприятной ситуации небезопасно. Рассмотрим подход к решению проблемы безопасности общества, состоящего из Прогрессистов.

Определение 2. Неограниченное множество благоприятных ситуаций называется благоприятной средой.

Определение 3. Регулярное изменение ситуации означает, что для любого t существует будущий момент v (т.е. $v \geq t$), в который возникает поощрение s_v, определяемое согласно (1).

Утверждение 2. Чтобы обеспечить смысл жизни Прогрессиста в благоприятной среде, необходимо и достаточно регулярного изменения ситуации.

Доказательство. Докажем необходимость от противного. Предположим, что есть только одна благоприятная ситуация, и жизнь Прогрессиста имеет смысл, когда эта ситуация остается неизменной с момента o. Первичная и интегральная реакции на поощрение s_t, а также эмоции f_t показаны на рис. 1. После момента $o+\tau_2$ имеет место $n_t > y_t$ и Прогрессист постоянно испытывает отрицательные эмоции. Однако условие − утверждение 2 говорит о наличии смысла жизни Прогрессиста. Согласно условию (3), это означает, что существует v такое, что $v \geq t$ и $F(n_v, y_v) > 0$. Следовательно, предположение о неизменности ситуации противоречит условию−утверждение 2. Это противоречие доказывает необходимость.

Теперь докажем достаточность. Согласно определению 2, в благоприятной среде существует неограниченное множество благоприятных ситуаций. Таким образом, можно регулярно менять ситуацию, заменяя ее новой ситуацией из этого множества. В соответствии с определением 3, это означает, что для любого момента t существует v такое, что $v \geq t$, и в момент v возникает новое поощрение s_v, поэтому $y_t > n_t$ в интервале времени $(v+\tau_1, v+\tau_2)$ Таким образом, для любого t существует такое v, что $v \geq$ и $F(n_v, y_v) > 0$. Используя определение 1 для случая, когда АЭ является Прогрессистом, получаем, что его жизнь имеет смысл, что и требовалось доказать.

Содержательно, регулярное изменение ситуации инициирует новые позитивные входные воздействия, приводящие к получению положительных эмоций и дающие смысл жизни Прогрессиста. По сути, формируется эмоциональный ряд − временная последовательность положительных и отрицательных эмоций («белые» и «черные» полосы жизни). Такая последовательность, образованная цепочкой воздействий (1), называется Лестницей желаний. Очевидно, что для реализации Лестницы желаний в благоприятной среде необходимо и достаточно регулярно менять ситуацию. На рис. 2 показаны: a − первичная и b − интегральная реакции Прогрессиста на такую последовательность, а также c − его эмоции.

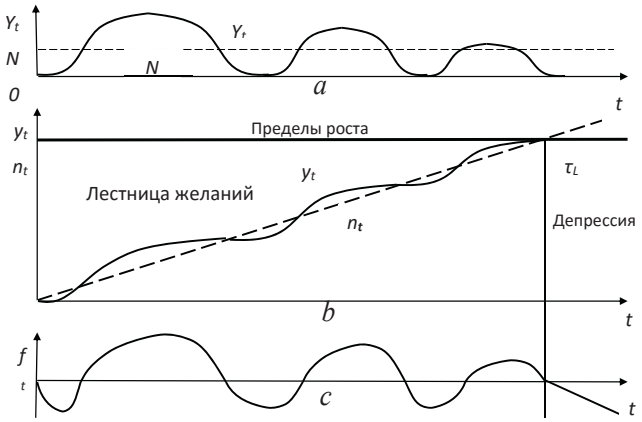


Рис. 2. Лестница желаний Прогрессиста

Следствие 1. Для существования смысла жизни Прогрессиста в благоприятной среде необходимо и достаточно его Лестницы желаний.

Доказательство. Согласно утверждению 2, для существования смысла жизни Прогрессиста в благоприятной среде необходимо и достаточно регулярно менять ситуацию. Но по определению это означает реализацию его Лестницы желаний, что и требовалось доказать.

Другими словами, при формировании Лестницы желаний Прогрессист всегда может рассчитывать на положительные эмоции в будущем, и его жизнь имеет смысл. Это гарантирует безопасность общества Прогрессистов. В свою очередь, для этого необходимо и достаточно создать последовательность поощрений, способствующих выполнению желаний каждого члена общества.

2.3. *Пределы потребления и социально-политическая нестабильность*

Прототипом Прогрессиста является «экономический человек», состояние которого определяется имеющимися деньгами. Соответственно, состояние Прогрессиста в обществе потребления определяется объемом его потребления. Цель такого Прогрессиста − увеличить потребление для удовольствий. Поэтому его можно называть Гедонистом.

Предположим, что потребление Гедониста в момент t характеризует величина y_t. Вследствие пределов роста, существует объективное ограничение потребления L (см. рис.2,*b*). С другой стороны, потребности Гедониста n_t постоянно растут (пунктирная линия на рис. 2,*b*). Предел роста L достигается в момент τ_L. После этого Гедонист не получает новых поощрений, и его жизнь не имеет смысла (утверждение 1). В результате Гедонист испытывает стойкие негативные эмоции, ведущие к депрессии (рис.2,*c*). Его недовольство обращается на власть и приводит к протестно-

му голосованию, политической нестабильности и др. Гнев и агрессия некоторых недовольных могут обратиться и на окружающих, и тогда общество потребления становится небезопасным.

Чтобы обеспечить политическую стабильность и общественную безопасность, нужно устранить причины массового недовольства членов общества. Традиционное решение заключается в расширении пределов роста L (например, рост потребления в результате нового технологического цикла Кондратьева). Альтернативное решение связано с либерализацией. Тогда активный Гедонист может изменить ситуацию, получив положительные эмоции и реализовав свою Лестницу желаний. Кроме того, он может получить власть и может изменить среду, предоставляя возможность избежать депрессии другим членам общества.

3. Модель и методы обеспечения социальной безопасности на основе страхов

3.1. Ощущения, эмоции и смысл жизни Фобика

Человеком управляют не только желания, но и страхи. Рассмотрим другой тип АЭ − Фобик. Его прототип − дальновидный человек, имеющий иррациональный страх, боязнь чего-то. Предположим, что в момент o Фобик подвергается негативному воздействию раздражителя (наказания) i_t

$$i_t = \begin{cases} i < 0, & if \quad o \le t \le o + e; \\ 0, & if \quad t < o \quad or \quad t > o + e. \end{cases} \qquad (4)$$

Сплошной линией на рис. 3,*a* показана первичная реакция Y_t на воздействие v как отрицательное ощущение. Сплошной линией на рис. 3,*b* показана вторичная интегральная реакция

$$y_t = \int_0^t Y_\tau d\tau,$$

на воздействие i_t. Пунктирные линии на рис. 3 показывают, соответственно, нейрофизиологическую норму N и нейропсихологическую норму

$$n_t = \int_o^t N d\tau = (t - o)N.$$

Эмоциональная функция Фобика, как АЭ, определяется согласно условию (2). На рис. 3,*c* показана кривая эмоций Фобика, связанных с воздействием i_t, рассчитанная по формуле (2).

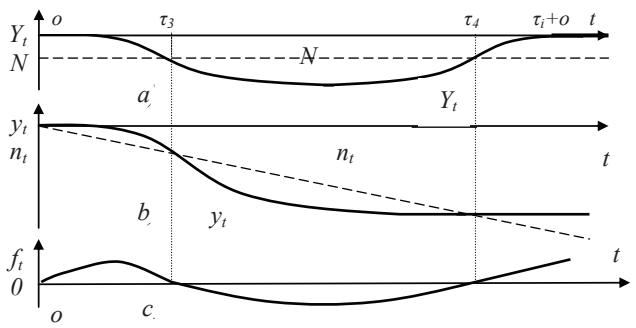


Рис. 3. Реакция Фобика на негативное внешнее воздействие − наказание i_t:
a – первичная; *b* – интегральная; *c* – эмоции
(τ_i − время адаптации к воздействию i_t)

Воздействие i_t (4) создает неблагоприятную ситуацию для Фобика. Среда, объединяющая множество неблагоприятных ситуаций, называется неблагоприятной средой.

Жизнь Фобика, как АЭ, имеет смысл при выполнении условия (3). На первый взгляд кажется, что жизнь Фобика в неблагоприятной ситуации связана с негативными эмоциями и не имеет смысла.

Утверждение 3. При неблагоприятной ситуации, жизнь Фобика имеет смысл.

Доказательство. Первичная и интегральная реакция на воздействие i_t, а также эмоции Фобика f_t показаны на рис. 3. Как видно на рис. 3,*b* и рис. 3,*c* для достаточно больших t, имеем $y_t > n_t$ и $F(n_t, y_t) > 0$. Таким образом, существует τ такое, что $\tau \ge t$ и имеет место $F(n_\tau, y_\tau) > 0$. Следовательно, выполняется условие (3). Используя определение 1 и учитывая, что АЭ − это Фобик, получаем, что жизнь Фобика имеет смысл, что и требовалось доказать.

Отметим, что из рис. 3,*c* видно, что негативные эмоции, связанные со страхом, проходят (вспомним слова царя Соломона). По существу, согласно утверждению 3, смысл жизни Фобика обусловлен отсутствием изменений − новых раздражителей, ведущих к неприятным ощущениям. Заметим, что нежелание таких изменений побуждает Фобика избегать любых действий, могущих вызвать новое раздражение. С этой точки зрения сообщество Фобиков безопасно.

3.2. Предотвращение трансформации Фобика в Прогрессиста

Прототип модели Фобика − человек, страдающий фобией, сохраняющий её, независимо от внешних факторов (даже если реальность опровергает фобию). Пример − психически больной человек. Но здоровый человек адаптируется к реальности. И если страхи, связанные с фобией, не подтвердятся, то со временем он забудет о них, и перестанет быть носителем фобии. Таким образом, адаптация в благоприятной среде приводит к забвению фобии. При этом человек, страдающий фобией, превращается в нормального человека. По сути, происходит превращение испуганного человека, стремящегося избежать раздражения, наказания, боли, в нормального человека, стремящегося к удовольствиям.

В частности, в обществе потребления Фобик превращается в Прогрессиста с постоянно растущим желанием удовольствий, т.е. в Гедониста (см. п.2.3). Достигнув пределов роста, такой Гедонист испытывает стойкие негативные эмоции и недовольство. Это ведет к нестабильности и угрожает общественной безопасности. Избежать этого можно, предотвратив трансформацию Фобика в Прогрессиста.

Утверждение 4. Предположим, что АЭ не забывает фобию в течение времени τ_f после окончания периода адаптации к воздействию (4), $\tau_f > 0$. Тогда, чтобы сохранить смысл жизни Фобика и предотвратить его превращение в Прогрессиста, достаточно регулярных воздействий (4) с интервалом времени $\tau_p = \tau_i + \tau_f$.

Доказательство. Чтобы предотвратить превращение Фобика в Прогрессиста, необходимо, чтобы АЭ не

забывал фобию. По условию утверждения 4 АЭ не забывает фобию в течение времени τ_f, τ_f>0, после окончания времени адаптации к воздействию (4). Далее, согласно рис. 3, время адаптации к воздействию равно τ_i. Поэтому, чтобы предотвратить превращение Фобика в Прогрессиста, достаточно регулярных воздействий (4) с интервалом времени $\tau_p=\tau_i+\tau_f$.

Покажем, что жизнь Фобика имеет смысл при таких воздействиях. На рис. 4 показаны соответствующие регулярные первичные и интегральные реакции, а также эмоции Фобика, вызываемые воздействиями (4). С учетом τ_f>0, из рис. 4 видно, что существует момент v>o, удовлетворяющий неравенствам $\tau_i+o<v<\tau_f+\tau_i+o$, при котором $F(n_v, y_v)$>0. Поскольку o может принимать любое допустимое значение, можно сформулировать общее утверждение: для любого момента w, в котором появилось воздействие (4), существует момент v>w, удовлетворяющий неравенствам $\tau_i+w<v<\tau_i+\tau_f+w$, такой, что $F(n_v, y_v)$>0. Следовательно, условие (3) выполняется. Таким образом, используя определение 1 и учитывая, что АЭ − это Фобик, получаем, что жизнь Фобика имеет смысл, что и требовалось доказать.

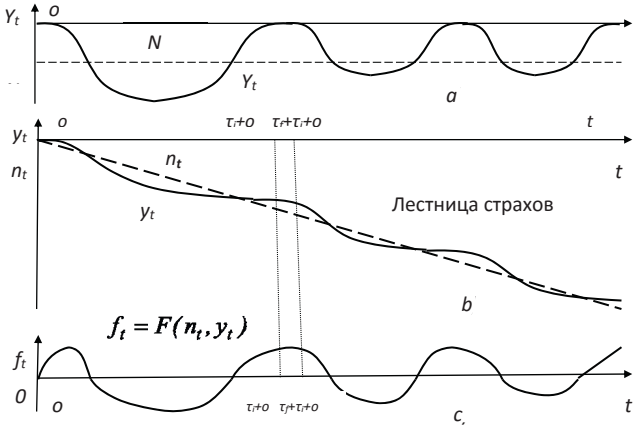


Рис. 4. Лестница страхов Фобика

Содержательно, регулярные неприятные воздействия (раздражения) не позволяют АЭ забыть о фобии. Как видно из рис. 4, они приводят к эмоциональному ряду − временной последовательности положительных и отрицательных эмоций («белые» и «черные» полосы жизни Фобика). Такая последовательность, образованная цепочкой воздействий (4), называется Лестницей страхов Фобика. Она придает смысл жизни Фобика даже в неблагоприятной среде, что обеспечивает стабильность и безопасность (например, при пределах роста в обществе потребления).

Как видно из рис. 4, если изменения в неблагоприятной среде происходят слишком часто, Фобик испытывает только негативные эмоции, и смысл его жизни отсутствует. Это побуждает Фобика протестовать против существующего порядка. Поэтому для поддержания фобии следует соблюдать условия утверждения 4.

3.3. Игры избирателей и политиков

Рассмотрим игры избирателей с политиком, отвечающим за безопасность общества в период между выборами. Если в момент выборов жизнь избирателя имеет смысл, он голосует за политика, в противном случае − против.

Рассмотрим цели и стратегии игроков в этих играх. Согласно принципу адекватности контролирующего субъекта контролируемому объекту, власти общества Прогрессистов должны также состоять из Прогрессистов. Поэтому сам политик должен быть Прогрессистом. Его состояние можно охарактеризовать количеством отданных за него голосов, рейтингов и т.д. Тогда смысл его жизни связан с реализацией собственной Лестницы желаний, положительные эмоции в которой связаны с очередным переизбранием. Для этого достаточно, чтобы во время выборов у каждого избирателя был смысл жизни.

Например, если общество состоит из Гедонистов, то и политик должен быть Гедонистом. При достижении пределов роста потребления Гедонист неизменно испытывает негативные эмоции, и смысл его жизни отсутствует (см. п.2.3). А поскольку избиратель-Гедонист считает власть ответственной за это, он будет регулярно голосовать против действующего политика. В этом случае жизнь политика-Гедониста также лишена смысла.

С другой стороны, если избиратель является Фобиком, он иногда испытывает положительные эмоции, если выполняются условия утверждения 4. Учитывая сказанное в п. 3.2, для того чтобы регулярно получать голоса АЭ, достаточно сделать из них Фобиков, а затем не допустить забывания фобии и трансформации их в Прогрессистов-Гедонистов. А для этого необходимо повторение воздействий-раздражений.

Утверждение 5. Политик-Гедонист, который создает Лестницы страхов для всех избирателей в обществе Фобиков, переизбирается и обеспечивает безопасность этого общества.

Доказательство. По условию утверждения 5 политик-Гедонист создает Лестницу страхов для каждого избирателя-Фобика. Для этого Политику нужно поддерживать их фобии путем регулярных раздражений-воздействий (4). Согласно утверждению 4, чтобы предотвратить превращение Фобика в Прогрессиста и сохранить смысл жизни Фобика, достаточно регулярных воздействий (4) с интервалом времени $\tau_p=\tau_i+\tau_f$.

Покажем, что найдется момент воздействия (4), при котором существует смысл жизни каждого Фобика в момент выборов u. Рассмотрим первичную и интегральную реакцию Фобика, а также его эмоции, инициируемые воздействием (4) в момент o. Эти реакции и эмоции показаны на рис. 4, начиная с момента o, в котором появилось раздражение. Из рис. 4 видно, что для любого момента o существует момент u>0, удовлетворяющий неравенствам $\tau_i+o<u<\tau_f+\tau_i+o$, таким, что $F(n_u, y_u)$>0.

Поэтому можно сформулировать общее утверждение: для любого момента w, в котором появилось раздражение, существует момент u, удовлетворяющий неравенствам $w+\tau_i<u<w+\tau_i+\tau_f$, такой, что u>w и $F(n_u, y_u)$>0. Отсюда следует, что для любого момента выборов u, удовлетворяющего неравенствам $w+\tau_i<u<w+\tau_i+\tau_f$, существует момент w, в котором появляется раздражение (4), такое, что $w<u$ и $F(n_u, y_u)$>0.

Отсюда, используя определение 1, получаем: для любого момента выборов *u*, Политик может выбрать момент воздействия (4), чтобы у каждого Фобика был смысл жизни в момент *u*. В этом случае Политик получает на выборах голоса всех Фобиков. А будучи избранным, Политик получает положительные эмоции и делает очередной шаг по своей Лестнице желаний. Это обеспечивает смысл жизни политика, как Гедониста. Таким образом, жизнь каждого элемента рассматриваемой социально-политической системы имеет смысл. Это обеспечивает общественную безопасность, что и требовалось доказать.

Утверждение 5 теоретически обосновывает традиционный рецепт манипуляции сознанием общества с помощью массового нагнетания страхов в период выборов. Поэтому политика-Гедониста, который строит Лестницу страхов для членов общества – Фобиков и Лестницу желаний – для себя, можно назвать Политиканом.

Регулярные воздействия-раздражения, генерируемые Политиканом, приводят к формированию Лестницы страхов Фобика. Такими раздражениями могут быть, например, информационные воздействия СМИ, подконтрольные Политикану. Для того, чтобы сделать их более убедительными, Политикан может регулярно организовывать всевозможные «утечки информации», инциденты и другие события, служащие поводами для напоминания о страхах, поддерживающих массовые фобии.

Политикан должен определить, когда применять раздражения (4), чтобы каждый Фобик имел смысл жизни во время выборов. Если раздражения так синхронизированы с выборами, то все Фобики голосуют за Политикана. При этом победитель выборов Политикан также испытывает положительные эмоции, реализуя собственную Лестницу желаний. Все это наполняет смыслом жизни Фобиков и Политикана даже в неблагоприятной среде, что приводит к общественной безопасности (даже в условиях пределов роста в обществе потребления).

Рассматриваемая модель полезна тем, что дает количественные рекомендации. Конечно, некоторые из приведенных выше выводов могут быть получены с помощью качественных рассуждений. Но математические формулировки не только строго обосновывают эти выводы, но и описывают неравенства относительно сроков воздействий на общество в рассматриваемой игре. Их формальное доказательство позволяет политику обосновать выбор моментов информационных воздействий, а избирателям предвидеть их.

Конечно, для принятия решений как политику, так и избирателям требуются значения параметров τ_1 и τ_2 (рис.1), τ_L (рис.2), τ_3 и τ_4 (рис.3), τ_i и τ_f (рис.4). Политик и избиратели могут получить их, обучаясь, например, на результатах специальных социологических исследований. Таким образом, выбирая момент воздействия в игре с избирателями, политик может использовать результаты как теоретического, так и эмпирического исследования. Подобное игровое обучение избирателей создает теоретическую и эмпирическую основу их решений.

4. Информационные технологии социальной безопасности

Пользуясь полученными теоретическими результатами, рассмотрим методы и информационные технологии обеспечения социально-политической стабильности и общественной безопасности.

4.1. *Фобии корпоративного психопата и токсичного лидера*

Рассмотрим поведение Фобика - модели человека, управляемого страхами в личных и производственных отношениях. Такой Фобик обеспечивает нужную ему последовательность положительных эмоций, создавая свою Лестницу страхов. Его фобии и эмоции могут усиливаться или ослабляться другими людьми. В личных отношениях Фобик строит свою Лестницу страхов, используя близких. Его страхи могут пугать близких, формировать их фобии и связанные с ними отрицательные и положительные эмоции.

Аналогичным образом при производственных отношениях Фобик строит свою Лестницу страхов в процессе взаимодействия с коллегами по работе. И, получив власть в корпорации, Фобик может строить свою Лестницу страхов, используя подчиненных. Чтобы понять, как Фобик может реализовать эту Лестницу страхов без явных конфликтов в корпорации, стоит вспомнить сюжет работы Ф. Кафки «Процесс» − постоянное нагнетание тревоги без предъявления обвинений. Ведь обычный клерк Джозеф К. обвиняется в преступлении, которое он не совершал, потому что он вообще ничего не совершал. Собственно, сами прокуроры не называют элементы преступления, так как они также не знают, в чем он виноват...

Вследствие такой активности, Фобик может превратиться в корпоративного психопата [5]. Заодно он может превратить подчиненных в Фобиков, руководствуясь принципами, основанными на утверждениях 3−5. По сути, его фобии передаются подчиненным, которые начинают строить свои Лестницы страхов, формирующие необходимые им самим последовательности положительных эмоций. Именно поэтому они следуют за корпоративным Фобиком, несмотря на то, что он является токсичным лидером [4]. Дальнейшее продвижение Фобика по иерархии облегчается, если корпорация находится в состоянии застоя. В конце концов, ее лидеры также постоянно опасаются негативных последствий пределов роста. Такой аллюр токсичных лидеров способствует распространению фобий не только в корпорациях, но и в обществах, и в странах, а через транснациональные корпорации токсичные лидеры выращиваются и во всем мире [4].

4.2. *Убедительность угроз и социальные фобии*

Ключевое значение для переизбрания Политикана имеет убедительность угроз, формирующих и поддерживающих массовые фобии. Для этого Политикан должен сделать угрозы максимально правдоподобными для электората. Могут быть написаны и реализованы самые смелые сценарии, которым, возможно, позавидовали бы лучшие сценаристы и режиссеры Голливуда. Рассмотрим убедительность разных видов угроз

при формировании социальных фобий такого рода. Наиболее убедительны угрозы, связанные со страхом смерти.

Фобия терроризма. После захвата заложников в Буденновске и особенно взрывов в Москве 9 сентября 1999 г. проблемы убедительности угрозы терроризма для россиян нет. После 11 сентября 2000 г., проблемы убедительности фобии террористической агрессии нет и для жителей Запада.

Фобии агрессии. Крупнейшим в мире военным альянсом является НАТО. Военный бюджет США больше, чем военный бюджет всех остальных стран мира, вместе взятых. Поэтому вероятность военной агрессии против стран Запада с применением обычных вооружений ничтожна. Соответственно, нет оснований для формирования фобии военной агрессии в обществах развитых стран Запада. Заметим, что проблемы убедительности военной угрозы в России нет. Ведь россияне помнят, что только от последнего вторжения фашистской Германии погибло 27 млн. граждан Советского Союза.

Рассмотрим проблему доверия к угрозе агрессии с использованием различных видов оружия массового поражения. Международные договора предусматривают создание специальных организаций и режимов для предотвращения использования оружия массового поражения - химического, токсинного, бактериологического (биологического) и ядерного. Информация об этих договорах, организациях и режимах публикуется Центром Джеймса Мартина [15]. Организационные модели и прогрессивные адаптивные механизмы функционирования международных режимов нераспространения химических, биологических и ядерных технологий двойного (военного и гражданского) назначения рассматривались в работе [16]. Само существование договоров, организаций и режимов, касающихся контроля над вооружениями, снижает убедительность социальных фобий, связанных с применением оружия массового поражения. Для переизбрания в этих условиях Политикан должен отыскать способы убеждения общества в реальности угроз, которые формируют и поддерживают массовые фобии.

4.3. *Пример: фобия ядерной войны*

Рассмотрим проблему убедительности угроз массового поражения на примере формирования и поддержания фобии ядерной войны. Ядерного угрозы для разных стран зависят от их военного потенциала. В частности, ядерные арсеналы США и России намного больше, чем других стран. Поэтому, например, угроза ядерного нападения Северной Кореи на США неубедительна, и не может использоваться для формирования и поддержания массовой фобии в американском электорате.

Таким образом, чтобы сформировать фобию, Политикан должен сделать ядерную угрозу реальной. Очевидно, что угроза ядерной войны тем более реальна, чем меньше договоров и соглашений, сдерживающих гонку ядерных вооружений. Прежде всего, это «Договор между США и СССР о ликвидации их ракет средней и меньшей дальности» (Договор о РСМД). Договор о РСМД был первым договором о сокращении ядерного оружия вместо установления потолка вооружений [15]. Это соглашение было заключено из-за сложности контроля запусков РСМД, поскольку возникло противоречие между максимально возможной скоростью реакции властей и необходимой скоростью принятия решений, определяющих судьбу народов, государств и всего человечества. Это противоречие впервые проявилось в 1980-х годах, когда страны Варшавского договора и НАТО развернули в Европе РСМД. Время их подлета к цели составляло всего несколько минут. Поэтому ни одна из сторон не имела физической возможности проверить информацию о запуске РСМД противника и провести переговоры.

В этих условиях, ответный удар должен был наноситься автоматически, а не по команде глав государств-противников. Такая система управления в СССР получила название «Периметр», а на Западе − «Мертвая рука» (“Dead Hand”). При этом вся система управления стала неустойчивой, поскольку любой сбой автоматики или помеха могли стать причиной мировой термоядерной войны. Эта угроза исчезла лишь после заключения в 1987г. Договора о РСМД, предусматривавшего полную ликвидацию РСМД.

В октябре 2018г. президент США Д.Трамп объявил о намерении выйти из Договора о РСМД. Теперь указанная угроза возникает вновь. При этом она многократно усиливается кибернетическими угрозами и оттого более реальна. Ведь успешная хакерская атака маньяка-одиночки на российскую или американскую компьютерную систему управления РСМД может стать причиной мировой термоядерной войны и гибели человечества.

В случае отказа США от Договора о РСМД начнется новая гонка ядерных вооружений. А поскольку любой шаг в этой гонке связан с новыми угрозами, то у Политикана появится реальная возможность регулярно поддерживать фобию ядерной войны для сохранения власти. Так человечество может стать заложником политических амбиций.

В будущем, после ликвидации Договора о РСМД, останется только «Договор между США и РФ о мерах по дальнейшему сокращению и ограничению стратегических наступательных вооружений» (Договор о СНВ). Это соглашение о сокращении ядерных вооружений между США и Россией устанавливает ограничение на развертывание стратегических боеголовок. Договор о СНВ действует до 5 февраля 2021 года, с возможностью продления на срок не более 5 лет (5 февраля 2026 года). В случае отказа и от Договора о СНВ начнется безудержная гонка ядерных вооружений. Таким образом, ядерная угроза станет еще более реальной. Поэтому, манипулируя информацией о новой повестке дня, Политикан будет легче поддерживать фобию ядерной войны у электората, а человечество станет еще ближе к гибели ...

4.4. *Пути разрешения основного противоречия*

В основе вышеописанных угроз и социальных фобий лежит противоречие между стремлением к росту материального потребления и пределами роста, об-

условленными ограничениями ресурсов и экологии биосферы (кратко – основное противоречие). Первый тип возможных решений основного противоречия основан на расширении пределов роста потребления (например, в результате нового технологического цикла Кондратьева) [13].

Второй тип решений связан с расширением пределов роста в одной или нескольких странах посредством их экономической, политической или военной экспансии в мире (например, путем организации цветных революций или локальных войн). Но такие решения подрывают международную стабильность и угрожают безопасности [14].

Третий тип решений связан с периодическим уменьшением макроэкономического потребления, за которым следует его рост (например, вследствие глобальных финансовых кризисов, распада государств и их союзов, межнациональных конфликтов). Такие решения также ведут к социально-политической и международной нестабильности [13,14].

По сути, вопросы, о которых мы говорим – протестное голосование, цветные революции, войны и т.д. - сами по себе не проблемы, а симптомы. Проблема заключается в продолжении материального роста в физически ограниченном мире. Постоянный рост потребления в конечном итоге достигнет уровня, который Земля просто не сможет обеспечить. Социально-политическая и международная нестабильность являются сигналами опасности, свидетельствующими о превышении физических возможностей планеты.

Поэтому принципиально иной класс решений основного противоречия связан с заменой парадигмы неограниченного роста материального потребления на парадигму нематериального, духовного развития. Разумеется, существует множество противников новой парадигмы [1]. Ведь, по сути, это смена идеологии общества потребления, затрагивающая весь «золотой миллиард». Кроме того, эта парадигма противоречит традиционным экономическим воззрениям, основанным на предположении, что непрерывный рост возможен и желателен. Большинство политиков также заинтересованы в росте, который решает проблемы безработицы, бедности, налогов и др.

Тем не менее, даже постепенная смена акцентов в идеологии потребления будет создавать новые возможности для позитивных изменений. Одно из них связано с активизацией творчества людей (особенно среднего класса развитых стран), направленного на духовное развитие. При этом растущие желания этих людей в духовной сфере могут быть удовлетворены без увеличения материального потребления. Для этого необходимы высокие гуманитарные технологии [11].

5. Заключение

Появление и развитие homo sapience на протяжении всей истории человечества было связано с прогрессистским сознанием, постоянным ростом желаний и возможностей людей. Сегодня человечество вступило в эру пределов роста из-за ограниченности ресурсов Земли, а также способности ее природы компенсировать вредные последствия деятельности человека. Это приводит к ограничениям роста и социально-экономической стагнации. Возникает противоречие между постоянно растущими желаниями человека с прогрессивным сознанием (Прогрессистом) и возможностями их удовлетворения. Его следствием является массовое недовольство в постмодернистском обществе потребления. Его члены считают, что власти должны обеспечить благоприятные условия для постоянного роста потребления. Поэтому их недовольство приводит к критике власти, что выражается в массовом протестном голосовании в странах Запада.

В этих условиях актуальны более глубокие исследования влияния человеческой природы, сознания, ощущений и эмоций на социально-политическую стабильность. Возможности для таких исследований создает быстрое развитие нейронаук. В соответствии с принятой концепцией, эмоциональные ожидания влияют на отношение АЭ к власти и обществу. Социально-политическая система, состоящая из АЭ, гарантированно стабильна, если все АЭ имеют позитивные ожидания. Показано, что прогрессистское сознание обеспечивает социально-политическую стабильность в благоприятной среде, создающей возможности для регулярного удовлетворения желаний каждого члена общества. Поэтому постмодернистское общество стабильно, пока возможности потребления не ограничены. С появлением пределов роста массы недовольных членов общества потребления угрожают социально-политической стабильности.

Людьми управляют не только желания, но и страхи. Показано, что массовые фобии могут способствовать общественной безопасности. Социально-политическая система, состоящая из общества Фобиков и Политика, стабильна в неблагоприятной ситуации. Но в отсутствие регулярных раздражителей фобия исчезает, и Фобики становятся Прогрессистами. В условиях пределов роста образованное из них общество становится небезопасным. Чтобы избежать этого, власть может поддерживать массовые фобии. Для этого требуется регулярно создавать информационные поводы, инциденты и другие события, нагнетающие страхи в обществе. Синхронизируя эти стимулы с выборами, Политикан в нужное время поддерживает позитивные ожидания Фобиков. Это является причиной их лояльности Политикану и его успеха на выборах. Примеры такого поведения политиков хорошо известны. Издавна шаманы и жрецы делали это, используя фобии внешнего врага, голода и т.д. Современные интриганы без этики широко используют подобные методы в глобальной политике, в частности, на основе русофобии.

Все эти проблемы являются следствием основного противоречия между увеличением потребления и пределами роста, вызванными ограничениями биосферы Земли. Кризис идеологии общества потребления создает возможности для позитивных изменений. Разные их виды возможны без экономического роста и многие из них ведут к более справедливому обществу и международной стабильности. В конце концов, необходимо заменить парадигму неограниченного роста материального потребления на парадигму нематери-

ального, духовного развития.

Желания и удачи привели к невиданному прогрессу человечества. Но нельзя дальше рисковать его выживанием, полагаясь исключительно на них.

Статья подготовлена по результатам исследований по проекту №16-19-10609 Российского научного фонда «Модели, методы и информационные технологии синтеза комплексных механизмов управления эргатическими активными системами».

Литература

1. Медоуз Донелла, Рандерс Й., Медоуз Д. Пределы роста: 30 лет спустя. – М.: Академкнига, 2007. - 342 с.
2. Kile F., Dimirovski G. Choices for global social stability. In: 17th IFAC World Congress Proceedings, pp. 6681-6685. COEX, Seoul, 2008.
3. Zakaria F. The Future of Freedom: Illiberal Democracy at Home and Abroad. New York: W.W. Norton, 2003.
4. Lipman-Blumen J. The allure of toxic leaders: why we follow destructive bosses and corrupt politicians – and how we can survive them. Oxford University Press, 2004.
5. Boddy C, Ladyshewsky R., Galvin P. Leaders without ethics in global business: corporate psychopaths. Journal of Public Affairs, 2010, №10, pp.121–138.
6. Цыганов В.В., Шульц В.Л. Олигархия: сущность, цикличность, модификации в условиях глобализации / Социологические исследования, 2009, №2, С.2-19.
7. Simon, H. Models of man - social and rational. John Wiley & Sons, Inc, New York, 1966.
8. Фрейд З. Введение в психоанализ – СПб: Азбука, 2016.- 326с.
9. Tversky A., Kahneman D. Advances in prospect theory: cumulative representation of uncertainty. Journal of Risk and Uncertainty 1992, №5, pp.297–323.
10. Fehr, E., Rangel, A. Neuroeconomic foundations of economic choice - recent advances. Journal of Economic Perspectives, 2011, № 25(4), pp.3-30.
11. Цыганов В.В. Адаптивные механизмы и высокие гуманитарные технологии. Теория гуманитарных систем. – М.: Академический проект, 2012. - 351с.
12. Цыганов В.В., Шульц В.Л. Высокие гуманитарные технологии в политической системе общества / Социологические исследования, 2012, №8, С.85-93.
13. Цыганов В.В., Шульц В.Л. Социология общественной безопасности. – М.: Наука, 2014. – 415с.
14. Tsyganov V. Limits of global growth, stagnation, creativity and international stability. Artificial Intelligence and Society, 2014, №29(2), pp.259–266.
15. James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies at Monterey Homepage, https://www.nti.org/learn/treaties-and-regimes/treaties/ (обращение 11.04.2019).
16. Цыганов В.В., Бородин В.А., Шишкин Г.Б. Интеллектуальное предприятие: механизмы овладения капиталом и властью. Теория и практика управления эволюцией организации. – М.: Университетская книга, 2004.-768с.

Материал поступил в редакцию 17.09.2019 г.

УДК 681.3

© Иванов М.А., Комаров Т.И., Саликов Е.А., Чепик Н.А.
© Ivanov M., Komarov T., Salikov E., Chepik N.

ХЕШ-ФУНКЦИЯ НА ОСНОВЕ 3D СТОХАСТИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

HASH FUNCTIONS BASED ON 3D STOCHASTIC TRANSFORMATIONS

Аннотация. *Хеш-функции наряду с генераторами псевдослучайных чисел являются базовыми элементами стохастических методов защиты информации, обеспечивающих непредсказуемое поведение средств и объектов защиты. Только на основе использования стохастических методов можно гарантировать защиту от активного противника.*

Предлагается алгоритм хеширования GDozenHash, основанный на использовании трехмерных стохастических преобразований Dozen+. Особенностью алгоритма является высокая степень параллелизма на уровне элементарных операций, иначе говоря, хеш-функция ориентирована на реализацию с использованием гибридных суперкомпьютерных технологий.

Целью данной работы является проектирование хеш-функции, ориентированной на реализацию с использованием гибридных суперкомпьютерных технологий.

Метод достижения цели заключается в использовании 3D стохастических преобразований Dozen+, особенностью которых является высокая степень параллелизма на уровне элементарных операций. Полученные результаты: представлено описание хеш-функции GDozenHash и результаты исследования статистической безопасности предлагаемого алгоритма хеширования.

Abstract. *Hash functions, alongside with pseudorandom number generators, are basic elements of stochastic information security techniques, which can provide unpredictable behavior of security methods or objects being protected. Stochastic techniques are the only methods capable of ensuring protection from an active intruder.*

A new GDozenHash hash algorithm based on Dozen+ 3D stochastic transformations is proposed. One of the features of the algorithm is a high parallelism of its elementary operations, i.e. this hash function can be implemented with hybrid supercomputer technologies in a simple way.

The purpose of the research is to develop a hash function capable of being implemented with hybrid supercomputer technologies.

The method: usage of Dozen+ 3D stochastic transformations, which feature a high parallelism of their elementary operations.The results obtained: GDozenHash hash function design and results of the analysis of its statistical security are presented.

Ключевые слова. *Хеш-функция, генератор псевдослучайных чисел, конструкция Sponge, 3D-стохастическое преобразование.*

Key words. *Hash function, pseudorandom number generator, sponge construction, 3D stochastic transformation.*

Введение

Стохастическими методами защиты информации (ЗИ) принято называть методы, основанные на внесении непредсказуемости в работу средств и объектов защиты. Термин «стохастический» применительно к задачам ЗИ впервые, по-видимому, стал применяться С.А. Осмоловским при построении кодов, обнаруживающих и исправляющих ошибки, возникающие при передаче данных по каналам связи [1]. Примеры использования стохастических методов ЗИ приведены в работах [1-5]. Только с использованием стохастических методов можно защититься от активного противника. Эффективность стохастических методов защиты определяется качеством используемых генераторов псевдослучайных чисел (ГПСЧ) и хеш-функций. Тенденцией последних лет стало массовое появление 2D и 3D стохастических преобразований [6-12].

Хеширование являются важным видом криптографического преобразования. Область применения хеш-функций чрезвычайно широка, они успешно решают практически все задачи защиты компьютерной информации от обеспечения аутентичности субъектов и объектов информационного взаимодействия до внесения неопределенности в работу средств и объектов защиты. При этом стоит отметить, что задача проектирования качественной хеш-функции более сложная, чем задача проектирования качественного симметричного шифра [13, 14].

Иванов Михаил Александрович *– доктор технических наук, профессор факультета Комплексной безопасности ТЭК, Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина, тел. 8 (926)558-60-99, E-mail:MAIvanov@mephi.ru;*
Комаров Тимофей Ильич *– аспирант, НИЯУ МИФИ;*
Саликов Евгений Александрович *– аспирант, НИЯУ МИФИ;*
Чепик Надежда Анатольевна *– аспирантка, НИЯУ МИФИ.*

Ivanov Mikhail *– doctor of technical sciences, professor at the department of Integrated safety of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (NRU), tel. 6(926)558-60-99, E-mail: MAIvanov@mephi.ru;*
Komarov Timofey *– postgraduate student, NRNU MEPhI;*
Salikov Evgeny *– postgraduate student, NRNU MEPhI;*
Chepik Nadezhda *– postgraduate student, NRNU MEPhI.*

Основы теории

Хеш-функция $h(x)$ – это функция, принимающая на входе в качестве аргумента информационную последовательность (прообраз) M произвольной длины и дающая на выходе в качестве результата $h(M)$ информационную последовательность (хеш-образ) фиксированной длины. Дадим формальное определение хеш-функции. Пусть $\{0, 1\}^m$ – множество всех двоичных строк длины m, $\{0, 1\}^*$ – множество всех двоичных строк конечной длины. Тогда хеш-функцией h называется преобразование вида h: $\{0, 1\}^* \rightarrow \{0, 1\}^m$, где m – разрядность хеш-образа.

Процесс получения хеш-функции можно рассматривать как наложение псевдослучайной последовательности (ПСП) на входную преобразуемую последовательность. Наиболее явно справедливость этого утверждения следует из анализа новой конструкции хеширования, получившей название Sponge [15, 16].

Любая криптографическая хеш-функция $h(x)$ должна удовлетворять следующим требованиям:

• хеш-образ $h(M)$ должен зависеть от всех бит прообраза M и от их взаимного расположения;

• при любом изменении M хеш-образ должен изменяться непредсказуемо, иначе говоря, в среднем должна измениться половина бит $h(M)$;

• хеш-функция должна быть односторонней (*one-way*), иначе говоря для произвольной n-разрядной строки $y \in \{0,1\}^n$ вычислительно сложно найти $x \in \{0,1\}^*$, такое, что $h(x)=y$(*pre-image resistance*);

• хеш-функция должна быть стойкой в смысле нахождения второго прообраза, иначе говоря, для заданной m-разрядной строки $x \in \{0,1\}^m$ вычислительно сложно найти произвольную строку $x' \in \{0,1\}^*$, $x' \neq x$ такую, что $h(x')=h(x)$ (*second pre-image resistance*);

• хеш-функция должна быть стойкой в смысле нахождения коллизий, иначе говоря, вычислительно сложно найти две произвольные строки x', $x'' \in \{0,1\}^*$, $x' \neq x''$ такие, что $h(x')=h(x'')$ (*collision resistance*).

Существуют два подхода к проектированию криптографической хеш-функции: проектирование «с нуля» и построение функции хеширования на основе использования функции зашифрования блочного шифра. Примером реализации первого подхода может являться хеш-функция MD5 – многолетний неофициальный мировой стандарт на функцию хеширования. Примером реализации второго подхода может являться хеш-функция Whirlpool, построенная на основе блочного шифра W [8].

Традиционная конструкция итерационной хеш-функции показана на рис. 1. Уравнение работы схемы при хешировании сообщения $M= M_1 M_2 M_3 ... M_n$, дополненного до длины, кратной разрядности блоков, имеет вид

$h_i=g(h_{i-1},M_i)$; i=1,2,3,...,n; $h_0=IV$; $h_n=h(M)$,

где $g(h_{i-1},M_i)$ − итерационная функция сжатия;

n – число блоков сообщения M;

IV – вектор инициализации.

Уравнение работы функции сжатия для одного из наиболее распространенных вариантов использования функции зашифрования

$E(K,M_\downarrow i)$:$\{0,1\}^\uparrow k \times \{0,1\}^\uparrow m (\{0,1\}^\uparrow m$ блочного шифра имеет вид

$g([h_\downarrow(i\text{-}1),M]_\downarrow i)=E(h_\downarrow(i\text{-}1),M_\downarrow i)(m_\downarrow i\ (h_\downarrow(i\text{-}1).$

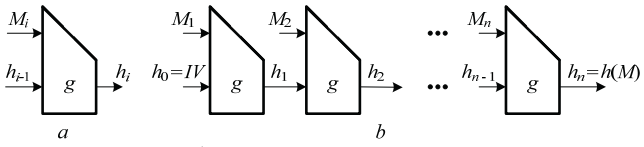


Рис. 1. Одна итерация алгоритма:
a – условное графическое обозначение итерации;
b – схема итерационной хеш-функции

Новые конструкции

Начиная с 2005 г. положение в области криптографических хеш-функций стало напоминать кризисное, и по этой причине в 2007 г. НИСТ объявил открытый международный конкурс по выбору нового стандарта хеширования SHA-3 [17]. Конкурс был ответом НИСТ на последние достижения в области криптоанализа алгоритмов хеширования. Среди функций, представленных на конкурс, помимо тех, которые имели традиционную конструкцию Narrow-Pipe, были представлены функции, имевшие новые конструкции, наиболее интересными из которых являются ChopMD, 3C и 3C+, Haifa, Wide-Pipe, Sponge.

На всех этапах конкурса в его работе активно участвовало мировое криптографическое сообщество. Основываясь на открытых комментариях, результатах криптоанализа, особенностей аппаратной и программной реализации, в октябре 2012 г. НИСТ объявил 3D алгоритм Keccak победителем, завершив пятилетний конкурс.

Итак, в качестве основы для нового стандарта SHA-3 была выбрана хеш-функция Keccak, построенная с использованием конструкции под названием Sponge (губка), которая показана на рис. 2. Схема Sponge имеет внутреннее состояние S разрядностью b, $b=r+c$, значение r называется *rate* (определяет скорость преобразования), а значение c (параметр безопасности) – *capacity*. Пусть RL(Resistance Level) – уровень безопасности, тогда по утверждению авторов конструкции справедливо соотношение $c \geq 2RL$ (иначе говоря, Sponge гарантирует нижнюю границу сложности $2^{c/2}$ любой атаки). Состояние делится на две части: S_1 разрядностью r и S_2 разрядностью c.

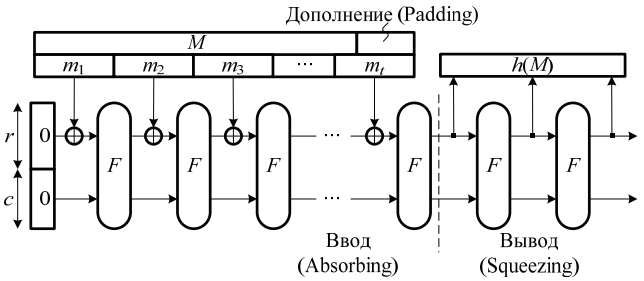


Рис. 2. Схема Sponge (в задаче хеширования данных)

Процесс хеширования состоит из двух многораундовых этапов: ввод (absorbing, впитывание) и вывод (squeezing, выжимание). Особенностью этапа ввода информации является то, что на каждом раунде блок сообщения складывается по модулю 2 только с частью состояния, а функция F производит преобразование всего состояния и делает его зависимым от все-

го сообщения *M*. На этапе вывода информации результат длины *b*, полученный на этапе впитывания, вновь подаётся на вход функции *F*. При этом с выхода этой функции считываются первые *r* бит. Этот процесс повторяется конечное число раз, при этом над *r* битами, считанными на каждом этапе, производится операция конкатенации (сцепления блоков). Повторение происходит до тех пор, пока не получим результат, т.е. хеш-образ, нужной длины.

Важно отметить, что функциональные возможности схемы Sponge значительно шире, чем только хеширование данных. На рис. 3 показаны два других варианта применения схемы Sponge.

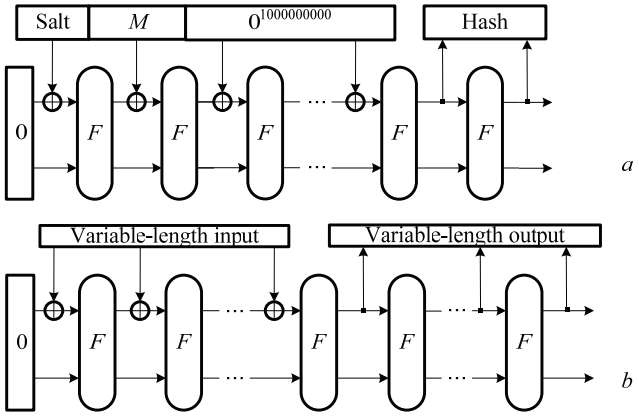


Рис.3. Два варианта использования схемы Sponge:
a – схема хеширования с солью и искусственным замедлением; *b* – преобразование входной последовательности произвольной длины в выходную последовательность произвольной длины

На рис. 3,*a* показана схема хеширования с солью (*salt*) и с замедлением, что целесообразно при организации парольных систем разграничения доступа и, в частности, для противодействия атакам с использованием радужных таблиц (*rainbow tables*). Использование входа и выхода переменной длины в схеме Sponge (рис. 3,b) может применяться, например, для генерации симметричных ключей из паролей. Другие варианты использования Sponge рассмотрены в работах [15, 16].

Схему Sponge можно изобразить по-другому, а именно так, как показано на рис. 4. После этого становится понятно, что схема не новая, иначе говоря, заслугой авторов Sponge является то, что они раскрыли многочисленные возможности этой схемы с точки зрения построения различных примитивов симметричной криптографии.

Алгоритм хеширования GDozenHash

Предлагается алгоритм хеширования GDozenHash на основе использования 3D стохастических преобразований Dozen+ [18]. Схема используемой функции Sponge (одной итерации алгоритма) показана на рис. 5. Главная особенность алгоритма – все входные и выходные блоки данных, все промежуточные результаты вычислений представляются в виде набора кубических массивов *S* байтов 4×4×4. Таким образом, результирующее преобразование обладает большой степенью параллелизма на уровне элементарных операций, иначе говоря, оно ориентировано на реализацию с использованием гибридных суперкомпьютерных технологий. Рекомендуемые значения разрядности хеш-образа и разрядности блоков сообщения:

$|h(M)| = |M_i| = 512$ бит.

Пусть входное состояние равно (S_3,S_2,S_1,S_0). Тогда последовательность преобразования (одна итерация алгоритма) имеет вид

1) ввод информации: $(S_3,S_2,S_1,S_0)=(S_3,S_2,S_1, S_0 \oplus M_i)$;

2) нелинейное преобразование каждого элемента S_i состояния по алгоритму Dozen+

(S_3,S_2,S_1,S_0)=(Dozen+(S_3); Dozen+(S_2); Dozen+(S_1); Dozen+(S_0));

3) линейное преобразование перемешивания состояния

$(S_3,S_2,S_1,S_0)=L^4(S_3,S_2,S_1,S_0)$,

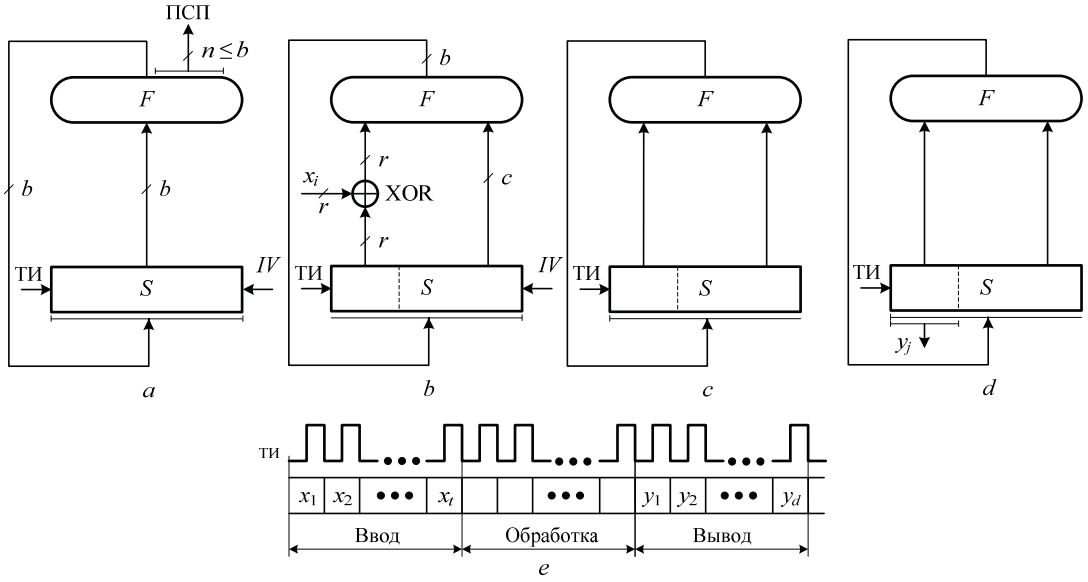


Рис.4. Схема Sponge (другой взгляд): *a* – ГПСЧ; *b* – схема преобразования в фазе ввода; *c* – схема преобразования в фазе обработки; *d* – схема преобразования в фазе вывода информации; *e* – временная диаграмма ввода, обработки входной и вывода выходной последовательностей;
ПСП – псевдослучайная последовательность; ТИ – тактовые импульсы; x_i, y_i – соответственно элементы входной и выходной последовательностей, i=1,…,t; j= ,…,d

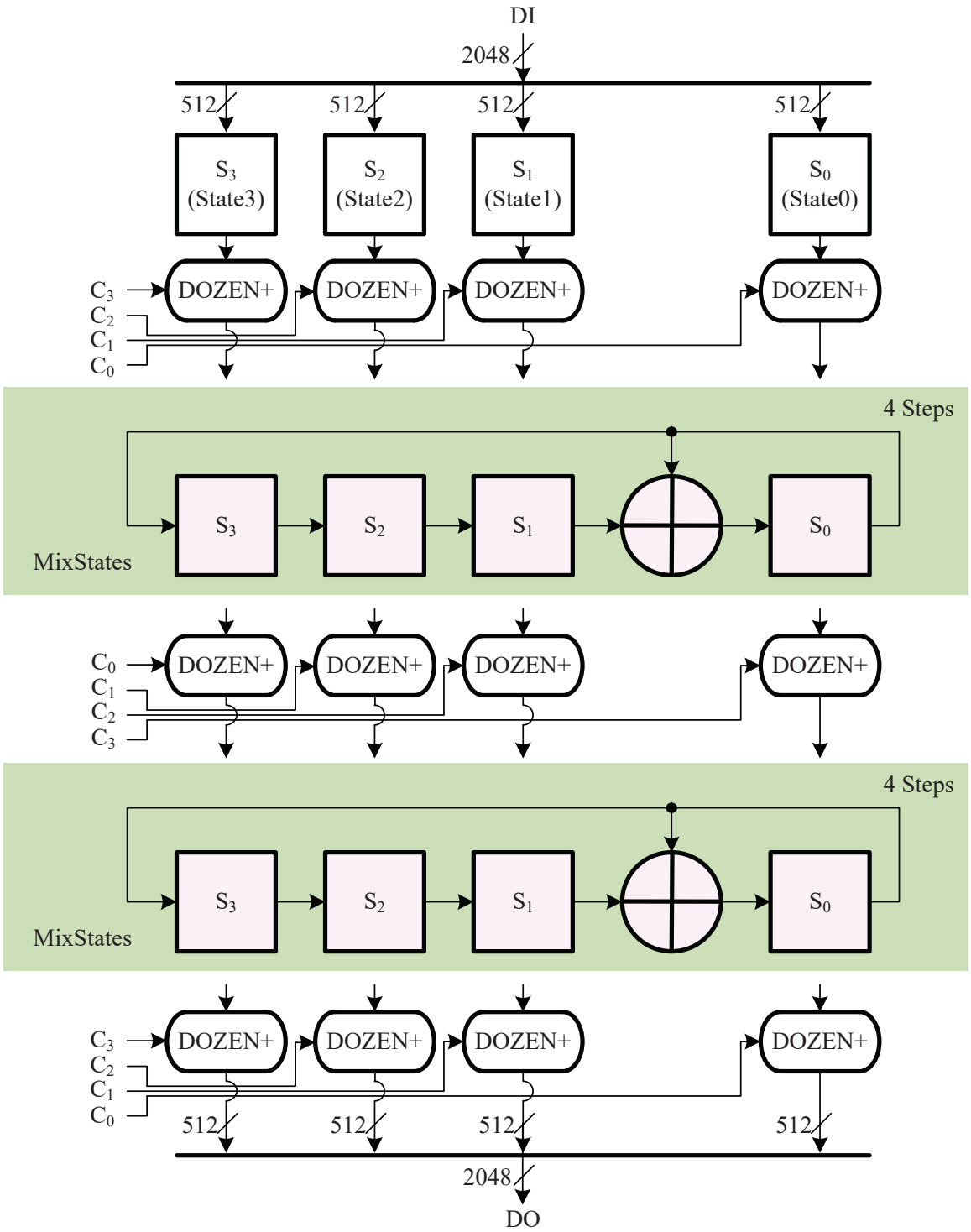


Рис.5. Функция Sponge алгоритма GDozenHash:
DI (DataInput) – входной блок данных; *DO* (DataOut) – выходной блок данных;
(S_3, S_2, S_1, S_0) – состояние алгоритма разрядностью $|S_3|+|S_2|+|S_1|+|S_0| = 4\times512=2048$ бит;
C_0 – константа 25h 41h 05h 0Ah 41h FFh 05h 0Ah 5Ah 59h 5Ah 0Ah A5h 77h 78h 25h;
C_1 – константа 6Ah 26h 22h C2h A5h 26h 22h C2h 41h 55h FFh 25h 55h 5Ah 20h 0Ah;
C_2 – константа 38h A5h 09h 38h 25h 41h 09h 38h A5h B8h 41h 09h 32h FFh 02h 20h;
C_3 – константа C2h 5Ah 25h 6Ah 5Ah A5h 25h 6Ah 25h 26h 05h 22h 19h 41h FFh 02h

где $L(S_3,S_2,S_1,S_0) = (S_3,S_2,S_1,S_0 \oplus S_1)$;

4) Нелинейное преобразование каждого элемента S_i состояния по алгоритму Dozen+

(S_3,S_2,S_1,S_0)=(Dozen+(S_3), Dozen+(S_2), Dozen+(S_1), Dozen+(S_0));

5) Линейное преобразование перемешивания состояния

$(S_3,S_2,S_1,S_0)=L^4(S_3,S_2,S_1,S_0)$;

6) Нелинейное преобразование каждого элемента S_i состояния по алгоритму Dozen+

(S_3,S_2,S_1,S_0)=(Dozen+(S_3), Dozen+(S_2), Dozen+(S_1), Dozen+(S_0)).

Выходное состояние (результат преобразования) равно (S_3,S_2,S_1,S_0).

При выполнении преобразования Dozen+(S) куб элемента состояния S делится на 4 слоя S_{x3}, S_{x2}, S_{x1}, S_{x0}

(квадратные массивы байтов 4×4) вдоль оси *x*, потом на 4 слоя S_{y3}, S_{y2}, S_{y1}, S_{y0} вдоль оси *y* и, наконец, на 4 слоя S_{z3}, S_{z2}, S_{z1}, S_{z0} вдоль оси *z*. Каждый слой подвергается перемешиванию с использованием преобразования MixLayer

MixLayer(S_{ij})=AddConst(MixState(SubBytes(S_{ij}))).

Пусть Q – строка состояния слоя Layer $|Q|$=128, Q=(Q_{16}…Q_1), $Q_i \in$GF(2^8), i =1,…,16. Тогда нелинейное преобразование SubBytes (замена байтов состояния слоя) определяется выражением

SubBytes(Q)=SubBytes(Q_{16}||…||Q_1)=

=SubByte(Q_{16})||…||SubByte(Q_1),

где SubByte(Q_i) – преобразование замены байта Q_i. Линейное преобразование MixState (перемешивания состояния слоя) на основе генератора псевдослучайных чисел, функционирующего в GF(2^8), построенного по схеме Галуа, определяется выражениями

MixState(Q)= $R^{16}(Q)$ = R^{16}(Q_{16}||…||Q_1)=

=($a_{16}Q_1$||Q_{16}+$a_{15}Q_1$||…||Q_2 + a_1Q_1)^{16} = QT^{16},

где все операции выполняются в поле GF(2^8);

$a_i \in$ GF(2^8) – коэффициенты характеристического полинома $\varphi(x)=a_{16}x^{16}+a_{15}x^{15}+a_{14}x^{14}+\ldots+a_2x^2+a_1x-1$, примитивного над GF($2^8$);

T – квадратная матрица 16×16 вида

$$\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ a_{16} & a_{15} & a_{14} & \ldots & a_2 & a_1 \end{pmatrix}.$$

Уравнения работы линейного преобразования R (умножения строки состояния слоя Q на T) имеют вид

$$\begin{cases} Q_j = Q_{j-1} + a_j Q_1, \; j = 1,\ldots,15; \\ Q_{16} = a_{16} Q_1. \end{cases}$$

Преобразование AddConst суть операция поразрядного XOR байтов состояния слоя с соответствующими байтами констант C_3,C_2, C_1, C_0.

Методика и результаты тестирования

Учитывая, что процесс хеширования можно рассматривать как наложение ПСП на входную последовательность *M,* в качестве методики тестирования алгоритма GDOZENHASH была выбрана методика статистического тестирования ПСП НИСТ [19], предполагающая использование большого числа оценочных тестов. Результаты тестирования при различном числе

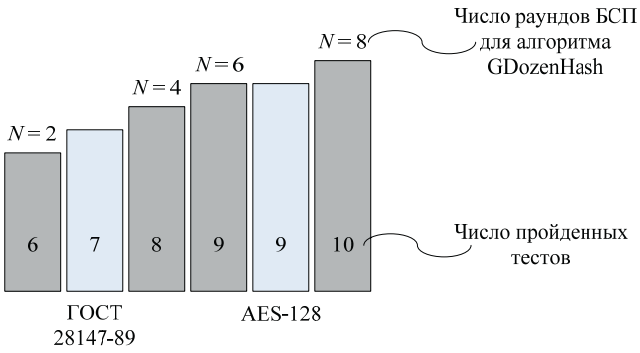


Рис.6. Число пройденных тестов НИСТ для генератора ПСП на основе алгоритмов ГОСТ 28147-89, AES-128 и GDozenHash для различного числа раундов базового стохастического преобразования (БСП)

итераций N базового стохастического преобразования (БСП) состояния (S_3,S_2,S_1,S_0), показанного на рис. 5, приведены на рис. 6. Таким образом, можно сделать вывод о статистической безопасности алгоритма.

Выводы

На основе использования 3D преобразований Dozen+ разработан алгоритм хеширования GDozenHash, обладающий высокой степенью параллелизма на уровне элементарных операций и ориентированный на реализацию с использованием гибридных суперкомпьютерных технологий. Тестирование алгоритма по методике НИСТ показало его статистическую безопасность. Направлением дальнейших исследований может являться разработка алгоритма хеширования на основе последовательной и параллельной композиции итерационных преобразований.

Литература

1. Осмоловский С.А. Стохастические методы передачи данных. М.: Радио и связь, 1991. 239 с.
2. Осмоловский С.А. Стохастические методы защиты информации. – М.: Радио и связь, 2003. 320 с.
3. V. Mao. Modern Cryptography. Theory and Practice. – Prentice Hall PTR, 2003.
4. M. Bellare, P. Rogaway. Optimal asymmetric encryption. In A. de Santis, editor, Advances in Cryptology – Proceedings of EUROCRYPT'94, Lecture Notes in Computer Science 950, pp. 92-111. Springer-Verlag, 1995.
5. Shai Halevi and Hugo Krawczyk. Strengthening Digital Signatures via Randomized Hashing. In Crypto '06, volume 4117 of LNCS, pages 41–59. Springer-Verlag, 2006.
6. Announcing the ADVANCED ENCRYPTION STANDARD (AES). Federal Information Processing Standards Publication 197, November 26, 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
7. Nakahara Jr., J.: 3D: A Three-Dimensional Block Cipher. In: Franklin M.K., Hui L.C.K., Wong D.S. (eds.) CANS 2008. LNCS, vol. 5339, pp. 252–267. Springer, Heidelberg (2008).
8. Barreto, V. Rijmen. The WHIRLPOOL Hashing Function., http://cryptospecs.googlecode.com/svn/trunk/hash/specs/whirlpool.pdf.
9. G. Bertoni, J. Daemen, M. Peeters, G. Van Assche. Keccak specifications, http://keccak.noekeon.org/Keccak-specifications-2.pdf.
10. Benadjila, R., Billet, O., Gilbert, H., Macario-Rat, G., Peyrin, T., Robshaw, M., Seurin, Y. SHA-3 proposal: ECHO. Submission to NIST (updated) (2009), http://crypto.rd.francetelecom.com/echo/doc/echo_description_1-5.pdf.
11. P. Gauravaram, L. R. Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schlaffer, and S. S. Thomsen. Grøstl – a SHA-3 candidate. Submission to NIST (Round 3), 2011. Available: http: //www.groestl.info.

12. Информационная технология. Криптографическая защита информации. Функция хеширования. ГОСТ Р 34.11-2012. – Москва, Стандартинформ, 2012.
13. Phillip Rogaway and Thomas Shrimpton. Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. In FSE '04, volume 3017 of LNCS, pages 371–388. SpringerVerlag, 2004.
14. S. Al-Kuwari, J. H. Davenport, R. J. Bradford. Cryptographic Hash Functions: Recent Design Trends and Security Notions. Short Paper Proceedings of 6th China International Conference on Information Security and Cryptology (Inscrypt '10). 2010, Science Press of China, pp. 133-150.
15. G. Bertoni, J. Daemen, M. Peeters, G. Van Assche. Sponge functions. Ecrypt Hash Workshop, Barcelona, Spain, May 2007. http://sponge.noekeon.org/.
16. G. Bertoni, J. Daemen, M. Peeters, G. Van Assche. Permutation-based encryption, authentication and authenticated encryption. http://keccak.noekeon.org/KeccakDIAC2012.pdf.
17. National Institute of Standards and Technology. Announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (SHA-3) Family, 2007. (volume 72, pages 62212–62220).
18. Иванов М.А., Матвейчиков И.В., Скитев А.А. Три новых способа стохастического преобразования данных. Труды Международной конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий» (REDS-2016), Moscow, Russia, May 25-26, pp. 351-355.
19. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22b.pdf.

Материал поступил в редакцию 17.06.2019 г.

УДК 316.4

© Силантьев А.Ю., Гриняев С.Н.

© Silantyev A., Grinyaev S.

КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ СОЦИАЛЬНЫХ СИСТЕМ

COMPREHENSIVE SOCIAL SECURITY

Аннотация. *В статье анализируется понятие комплексной безопасности в приложении к социальным системам. За основу анализа принято представление о социальной системе как объекте, обладающем жизненным циклом и целевой функцией выживания в изменяющихся условиях. Обсуждаются основы анализа комплексной безопасности. Приводятся примеры проблем комплексной безопасности глобальных систем.*

Abstract. *The article analyzes the concept of comprehensive security as applied to social systems. The analysis is based on the idea of a social system as an object that has a life cycle and a survival function in changing conditions. The basics of comprehensive security analysis are discussed. Examples of the problems of comprehensive security of global systems are given.*

Ключевые слова. *Социальная система, жизненный цикл, комплексная безопасность.*

Key words. *Social system, life cycle, comprehensive security.*

Введение

Термины

Система – структурированный объект и/или множество связанных объектов.

Состояние системы – совокупность её структур и процессов.

Жизнь – воспроизводящаяся условная информация, определяющая структуру и поведение объектов (систем).

Разум – адаптация (модификация) живых объектов (систем) к изменяющимся условиям.

Социальная система (объект) – обладающий разумом живой организм, включающий человека.

Жизненный цикл – последовательные состояния (рождение, размножение, гибель, трансформация) и процессы системы, характеризующиеся существенным изменением структуры и/или накопившейся условной информации.

Опасность – угроза потери жизни (разрушения условной информации, структуры и/или процессов системы) или неприемлемого отклонения от заданного жизненного цикла.

Гибридная опасность – многоаспектная опасность.

Кризис – системная опасность, опасность для всех системных объектов (агентов).

Безопасность – отсутствие опасности, наличие защиты от опасности.

Комплексная безопасность – многоаспектная, обладающая полнотой (ко всем видам угроз – простым, гибридным и системным) безопасность.

Задача статьи обозначить смысл и цели *комплексной безопасности социальных систем*, а также определить инструменты ее научного анализа. Авторское понимание терминов, использованных в статье, представлено в разделе Термины. Обсуждение терминов можно найти в работах [1–8].

Объект исследования – *социальные системы*. Представление о социальных системах как живых изменяющихся организмах развито в работе [7]. Согласно этому представлению любые социальные системы (и их элементы) могут рассматриваться как объекты (агенты), обладающие ценностями (целевыми предпочтениями) и структурированными ресурсами (условной информацией), которые в совокупности и определяют процессы, протекающие в системе.

Особенностью социальных систем является участие человека (субъекта) во всех значимых целевых процессах. Поэтому динамика социальных процессов зависит не только от *материальной структуры* системы, но и от ее *информационного наполнения*.

При анализе систем необходимо учитывать информированность и рефлексию субъектов (способность воспринимать и реагировать на поступающую информацию). Информация при этом носит условный характер (зависит от способа донесения и восприятия) и обрабатывается субъективно (разумно, в интересах и в зависимости от состояния субъекта).

Социальные системы иерархичны (дифференцируются на объекты (агенты) разных структурных уровней) и образуют сети. Поведение системных агентов

Силантьев Альберт Юрьевич *– доктор технических наук, профессор, РГУ нефти и газа (НИУ) им. И.М.Губкина, e-mail: aysilantev@gmail.com, тел.8(925)008-3-90;*

Гриняев Сергей Николаевич *– доктор технических наук, старший научный сотрудник, декан факультета комплексной безопасности топливно-энергетического комплекса, РГУ Нефти и Газа (НИУ) им. И.М. Губкина,e-mail: gsn@gubkin.pro, тел.8(916)633-75-33.*

Silantiev Albert *– doctor of technical sciences, professor, I.M. Gubkin Russian State University of Oil and Gas (NRU), e-mail: aysilantev@gmail.com, tel. 8(925)008-3-90;*

Grinyaev Sergey *– doctor of technical sciences, senior researcher, dean of the faculty of comprehensive security of the fuel and energy complex, I.M. Gubkin Russian State University of Oil and Gas (NRU), e-mail: gsn@gubkin.pro, tel. 8(916)633-75-33.*

также субъективно и зависит от поступающей условной информации и их состояния.

Комплексная безопасность

Предмет исследования – *комплексная безопасность* социальных систем (её агентов). Этимология комплексной безопасности на примере объектов топливно-энергетического комплекса рассмотрена в работе [8]. В частности, понятие опасности связывается с наличием угроз документированным процессам объекта.

Угрозы по своему характеру бывают частными (один процесс), гибридными (много связанных процессов) и системными (все процессы агента). Комплексная безопасность подразумевает отсутствие или возможность парирования всех видов угроз.

Жизненный цикл социальной системы.

В нашем понимании основой идентификации опасности (угроз) является самооценка текущего и прогнозного состояний (системных процессов) агента. Самооценка состояния может быть построена на представление о жизненном цикле (прогнозной целевой структуре и процессах системы, см. рисунок).

Системные процессы зависят от вида объекта (целевого назначения) и его иерархии (структур). По видам целевых процессов среди частных угроз можно выделить: властные (управление – право), экономические (производство – финансы – товар – деньги), ментальные (идеология – воспитание, наука – технологии) и социальные (индивид – семья – общество). Более полное перечисление социальных процессов и соответствующих им угроз можно найти в работе [7].

Социальная система по определению является сложной системой, не допускающей полного (исчерпывающего) описания, так как на ее поведение влияют слабые субъективные факторы (состояния отдельных людей), которые способны изменять понятийное пространство состояний системы. Тем не менее, при анализе жизненного цикла системы можно выделить основные процессы, которые определяют устойчивость и безопасность ее развития.

Жизненный цикл социальной системы (см. рисунок) состоит из рождения, экстенсивного развития, кризисов и трансформации (интенсивного развития или смерти).

Комплексная безопасность имеет изменяющийся приоритет и значение в разные периоды жизненного цикла систем. Значимость ее возрастает в кризисные периоды и может стать первичной в период интенсивного развития (преобразования), когда система находится в зоне максимального риска и множественных системных угроз (бифуркация между модификацией и смертью).

Рождение – это период построения (создания системы) на основе имеющейся генетической (условной информации). Например, для предприятия это период строительства и ввода в эксплуатацию в соответствии с проектной и нормативной документацией, территориальными и федеральными законами и другими ограничениями. Имеющаяся нормативная и проектная документация (условная информация) определяет лишь порядок и приоритетность процессов, но сами процессы реализуются в соответствии с текущей ситуацией и возможностями.

Угрозами на этом этапе существования системы будут риски, способные остановить развитие зародыша (строительство) до момента полноценного развития (ввода в эксплуатацию). Перечислим некоторые характерные риски. Властные риски – изменение законодательства (об отводе земли, о правилах природопользования, об экологической безопасности), политические ограничения на ввоз оборудования и технологий, административные препоны, санкции. Экономические риски – разорение спонсора или кредитора строительства, резкое изменение курсовой стоимости валюты и целевых рынков, отказ ключевых поставщиков. Ментальные риски – протесты населения, недоработка или отрицательные результаты испытаний новых технологий, конкурентное противодействие в СМИ. Население – отсутствие кадров, тяжелые условия проживания, ограничения на виды деятельности.

В период рождения относительная роль собственных процессов обеспечения безопасности низкая, так как система находится в условиях поддержки и избытка ресурсов. Безопасность реализуется через генетически накопленную информацию (апробированные способы решения проблем).

Экстенсивное развитие – период, когда образец системы создан и действует. Системных ограничений по ресурсам или иного характера нет. Целевые задачи – тиражирование системы (основная задача жизни) и освоение ресурсного ареала.

Для предприятия период характеризуется устойчивым протеканием внутренних процессов. Критические риски в основном макросистемные.

Внешние угрозы. Властные – санкции, коррупция, правовые конфликты собственников. Экономические – конкуренция за вывод товаров на рынок, налоги, рост стоимости комплектующих и затрат на персонал. Ментальные – появление новых технологий, информацион-

ная конкуренция. Социальные - кадровое обеспечение, протесты рабочих, социальная нестабильность.

Внутренние угрозы. Технологические – соблюдение технологических норм и норм безопасности, обеспечивающих стабильную работу оборудования. Экономические - внутренний учет движения материалов и денежных средств. Управление – согласование производственных процессов. Ментальные – формирование парадигмы развития (миссии предприятия).

Значимость процессов обеспечения безопасности стабилизируется на уровне признания общесистемной важности. Инструменты обеспечения безопасности типовые (развиваются и тиражируются в рамках макросистемы).

Кризис – период накопления нерешенных системных проблем, достижение пределов развития (рост влияния ограничивающих факторов). Целевые задачи – удержание системы в состоянии существования (балансирование на грани допустимых состояний) с максимальным использованием имеющихся средств реагирования. Роль процессов безопасности возрастает. Методы обеспечения безопасности становятся индивидуальными для конкретной системы и учитывают ее особенности.

В этот период усиливается конкуренция между однотипными социальными агентами за ресурсы. Начинается их гибель и снижение численности (предприятия попадают в зону высоких рисков и разоряются). Возникает потребность в модификации (диверсификации, целевой переориентации) объектов. Растет (максимизируется) доля ресурсов, направляемых на безопасность (выживание) и поиск новых форм существования.

Интенсивное развитие – период поиска и апробации решений по выходу из кризиса. Задача периода – модификация внутренней условной информации, поиск и апробация нового решения для развития. Период множественных рисков и массовой гибели модифицируемых систем. Роль процессов безопасности максимальна, но ресурсы, отпускаемые на ее реализацию, сокращаются. Требуется оптимизация затрат на безопасность (максимум эффекта при минимуме затрат), появляются новые адаптивные средства обеспечения безопасности.

Окончание периода интенсивного развития характеризуется положительным разрешением кризиса и формированием перспективной системы (нового набора условной информации), обладающей возможностями роста и тиражирования.

Период отличается высокой концентрацией ресурсов безопасности при катастрофическом снижении их общего объема.

Для каждого периода жизненного цикла системы характерны свои угрозы и способы обеспечения безопасности. При этом понятие комплексности в период экстенсивного развития (безопасность для всех) будет отличаться от понятия комплексности в период кризиса (все виды безопасности для перспективных (избранных) модификаций).

Если рассматривать современную мировую социально-экономическую систему, то политические решения о денонсировании США ряда международных договоров по сотрудничеству и безопасности (ПРО, РСМД, торговля оружием) является проявлением понимания кризисных процессов, происходящих в США и мире, и переход к обеспечению собственной безопасности вне общего мирового контекста.

Методы исследования комплексной безопасности

Выбор методов исследования очень важен, так как, выбирая определенный математический аппарат, мы сужаем наше возможное представление о предметной области до понятий и конструкций этого аппарата.

Какие бывают методы? Если рассматривать наиболее распространенные математические методы, то они делятся по трем признакам (в соответствии с определением используемых в них понятий): стационарные – динамические, дискретные – непрерывные, детерминированные – стохастические. Ни один из этих признаков не является исключительным для описания комплексной безопасности. Любой из математических методов может быть применен в зависимости от специфики конкретной задачи.

Однако существенными особенностями комплексной безопасности является зависимость от жизненного цикла рассматриваемой системы и участие людей в ключевых процессах.

Первое позволяет нам выбрать системный анализ в качестве инструмента анализа [9,10]. А второе заставляет рассматривать объекты комплексной безопасности как социальные организмы [7,11]. Системный анализ включает не только пассивное описание динамики систем, но и управление жизненным циклом и изменениями [10]. Теоретическое исследование процессов управления в социальных системах начинается с модификации классической теории управления (теории игр) [12-13], связанной с адаптивным изменением правил игры (критериев эффективности). Это теория активных систем [14] и теория управления организационными системами [15-17].

Ограниченность этих направлений заключается в фиксированности пространства эффективности (фиксированы понятия, в рамках которых формулируются критерии), что не позволяет моделировать выход из кризисных ситуаций и исследовать весь жизненный цикл систем. Содержательная динамика критериев с изменением их качественного состава (ценностей) исследуется в рамках теории социальных организмов [18].

Особенностью изучения социальных систем является одновременное наличие объективных фактов и субъективных мнений. Если объективные факты допускают оценки в рамках стандартных количественных метрик, то субъективные мнения описываются качественно и часто в слабо пересекающихся понятиях. Для их описания используют менее распространенные математические инструменты, такие как теория множеств или Р-адический анализ.

Подтверждение полученных результатов требует проведения как верификации (для объективных процессов), так и валидации (для субъективных процес-

сов). Это усложняет исследование, но выход можно найти в использовании методов экспертного анализа и переводе субъективных мнений в стандартные количественные метрики.

Ниже приведем несколько примеров вербальной постановки задач анализа комплексной (системной) безопасности.

Проблема перенаселения Земли и дисбалансов развития

Социальный объект – человечество. Системная угроза – неприемлемое снижение качества жизни в результате роста численности населения, дисбалансов развития, ограничений ресурсов и среды обитания. За ними последуют обострение социального недовольства и противостояние политико-экономических группировок. Этой проблеме посвящены работы [19,20], где рассматриваются различные виды социально-экономических ловушек, возникающих на пути современного развития, – сырьевая, средних доходов, инновационной отсталости, финансовой слабости, демографическая, имущественного неравенства, деидеологизации, деградации элит.

Проблема глобальных конфликтов и гибели современных цивилизаций

Социальный объект – человечество. Системная угроза – ядерное оружие, оружие массового уничтожения. Работ и согласованных действий (международных соглашений) по этому направлению много (см. [21-23]). Впервые столкнувшись с угрозой всеобщего уничтожения, человечество ответственно отнеслось к возникшей угрозе. Был заключен (или рассматривались) ряд международных соглашений (Договор о нераспространении ядерного оружия (1970), Договор о всеобъемлющем запрещении ядерных испытаний (1996), Договор о запрещении ядерного оружия (2017), Договор о ракетах средней и малой дальности (1987), Договор о стратегических наступательных вооружениях СНВ-1 (1991), СНВ-2(1993), СНП (2003), СНВ-3(2010)), которые позволили относительно спокойно существовать последние 50 лет. Однако новый системный кризис, обострivший проблему конкуренции цивилизаций и изменяющий ядерный мировой баланс, возвращает нас к временам, когда ядерное оружие уже на новом витке своего развития становится реальной угрозой всеобщей безопасности.

Проблема развития мировой либеральной экономической системы

Социальный объект – мировая экономическая и торговая системы. Системная угроза – рост диспропорций между регионами и агентами системы, избыточная концентрация ресурсов в отвлеченных структурах, не направленных на развитие технологий и экономики [7]. Либеральная система эффективна на этапах зарождения и роста экономики, но становится тормозом и наращивает социальную напряженность на этапах системных ограничений и кризисов.

Проблема социально-экономической политики развития России

Социальный объект – Россия. Системная угроза – низкие темпы экономического и технологического развития, угрожающие зависимостью от мировых рынков и политики мировых лидеров, с последующей потерей суверенитета [7,20,24]. Изменение внутренней либеральной социально-экономической политики необходимо для согласования интересов всех слоев населения, увеличения темпов роста и инноваций экономики, конкурентного и независимого позиционирования в изменяющейся мировой политико-экономической системе.

Проблема интеграции искусственного интеллекта

Социальный объект – человечество. Системная угроза – потеря человечеством лидерства в ареале собственного существования. Включение искусственного интеллекта в социальные процессы угрожает потерей человечеством «безусловного права» на доминирование в биосфере Земли. Разрешение вопроса , «является ли это угрозой или необходимым условием развития жизни?», требует системного исследования и целевого прогноза развития человечества [24-26].

Проблема генетических мутаций

Социальный объект – человек. Системная угроза – разрушение генетической информации, обеспечивающей продолжение рода. Низкая стоимость и условная простота изменений создают высокие риски неоправданно частых мутаций, что может привести к высокой смертности и снижению адаптационных возможностей [27-28]. Использование новых лекарственных средств и продуктов питания может привести к отложенной (в рамках нескольких поколений) системной реакции. Проблема требует тщательно контролируемого консервативного подхода к генетическим исследованиям.

Выводы

Комплексная безопасность требует рассмотрения угроз системного характера, способных привести к гибели объектов или недопустимым нарушениям процессов. Состав угроз зависит от этапов жизненного цикла и специфики объектов. В качестве инструмента моделирования и изучения комплексной безопасности предлагается использовать системный анализ, дополненный математическими моделями, построенными на иерархически и функционально структурированных сетях.

Современный кризисный этап трансформации человечества содержит ряд угроз системного характера, которые требуют изучения и адекватного реагирования. Контроль этих процессов является необходимым условием дальнейшего существования и развития.

Литература

1. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка. – М.: Азбуковник, 1997. – 944 с.

2. Ефремова Т.Ф. Новый словарь русского языка. Толково-образовательный. – М.: Русский язык, 2000. – 1209 с.
3. Нечаев В.И., Михайлушкин П.В. Экономический словарь: Справочное издание. – Краснодар: «Атри», 2011. – 464 с.
4. Тезаурус русской деловой лексики: http://rus-yaz.niv.ru/
5. Жеребило Т.В. Словарь лингвистических терминов. – Назрань: «Пилигрим», 2010. – 486 с.
6. Словарь русских синонимов: http://edbi.ru/
7. Силантьев А.Ю. Социальные законы и мировая модель развития. – М.: АНО ЦСОиП, 2019. – 248 с.
8. Гриняев С.Н., Правиков Д.И., Медведев Д.А. Комплексная безопасность ТЭК как объект научного анализа // Современная наука: Актуальные проблемы теории и практики. Естественные и технические науки, № 3/2, 2019, с. 24-30.
9. Системный анализ и принятие решений: словарь справочник. Под ред. Волковой В.Н., Козлова В.Н. – М.: Высшая школа, 2004. – 616 с.
10. Лоусон Г.Б. Путешествие по системному ландшафту. Под ред. Батоврина В.К. – М.:ДМК Пресс, 2013. – 370 с.
11. Жмеренецкий В.Ф., Летуновский В.В., Полулях К.Д. Теория безопасности социальных систем. – М.: НОУ МПСИ, 2010. – 182 с.
12. Вагнер Г. Основы исследования операций. – М.: Мир,1972. Т.1-3.
13. Гермейер Ю.Б. Игры с непротивоположными интересами.– М.: Наука, 1976.– 327 с.
14. Бурков В.Н. Основы математической теории активных систем. – М.: Наука,1977. – 255 с.
15. Бурков В.Н., Буркова И.В., Горгидзе И.А., Джавахадзе Г.С., Хуродзе Р.А., Щепкин А.В. Задачи управления в социальных и экономических системах. – М.: СИНТЕГ, 2005. – 256 с.
16. Новиков Д.А. Теория управления организационными системами. – М.: Издательство физико-математической литературы, 2007. – 584 с.
17. Бурков В.Н., Коргин Н.А., Новиков Д.А. Введение в теорию управления организационными системами.– М.: кн.дом «ЛИБРОКОМ», 2009. – 264 с.
18. Силантьев А.Ю. Методы теории социальных организмов. Системные проблемы качества, математического моделирования, информационных иэлектронных технологий. Ч.2. Социально-экономические системы. М.: Радио и связь, 2003. – с. 56-64.
19. Садовничий В.А., Акаев А.А., Коротаев А.В., Малков С.Ю., Соколов В.Н. Анализ и моделирование мировой и страновой динамики. – М.: ЛЕНАНД, 2017. – 352 с.
20. Малков С.Ю., Андреев А.И., Гринин Л.Е., Коротаев А.В.,Малков А.С. Россия в контексте мировой динамики. Моделирование и прогноз. М: - Учитель, 2016. – 208 с.
21. Андрюшин И.А., Чернышев А.К., Юдин Ю.А. Укрощение ядра: страницы истории ядерного оружия и ядерной инфраструктуры СССР. – Саров, Саранск: Красный октябрь, 2003. – 481 с.
22. Ядерное нераспространение. Учебное пособие, в 2 томах. Под ред. Орлова В.А. М.: ПИР-Центр, 2002. – 528 с.
23. Оскольская Д.И. Ядерное оружие как угроза глобальной безопасности в начале XXI века. XII международная конференция «Постбиполярный мир: проблемы безопасности евроазиатского геостратегического пространства». Архонт, №2(5), 2018.
24. Чернавский Д.С., Агеев А.И., Буданов В.Г., Колесова Л.А., Курдюмов В.С., Олескин А.В., Щербаков А.В. Россия 2112. – М.: Грифон, 2017. – 92 с.
25. Соколова С.Н. Искусственный интеллект и безопасность общества. Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. №1, 2016, с.63-68.
26. Хусаинов Т., Слюсарев В. Коэволюция естественного и искусственного как условие сохранения жизненного мира человека. Проект 18-011-00335 при поддержке гранта РФФИ.
27. Райан Ф. Виролюция. М.: Ломоносовъ, 2016. – 312 с.
28. Кэррол Ш. Приспособится и выжить! ДНК как летопись эволюции. М.: Corpus, 2015. – 392 с.

Материал поступил в редакцию 17.09.2019 г.

УДК 004.8; 316.4

© Силантьев А.Ю.
© Silantyev A.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И БЕЗОПАСНОСТЬ ЧЕЛОВЕЧЕСТВА

ARTIFICIAL INTELLIGENCE AND HUMAN SECURITY

Аннотация. *В статье обсуждается взаимодействие человеческого социума и искусственного интеллекта. Рассматриваются роли искусственного интеллекта и человека в новом технологическом социуме. Анализируются «угрозы» со стороны искусственного интеллекта.*

Abstract. *The article discusses the interaction of human society and artificial intelligence. The roles of artificial intelligence and man in a new technological society are considered. The "threats" from the side of artificial intelligence are analyzed.*

Ключевые слова. *Социальная система, искусственный интеллект, комплексная безопасность.*

Key words. *Social system, life cycle, comprehensive security.*

Введение

Идея написать статью по искусственному интеллекту появилась как реакция на публикации [1-4], в которых высказываются опасения относительно безопасности человечества перед «всемогущим» искусственным интеллектом (Artificial Intelligence). Опасения авторов разумны (как адаптивная реакция на технологические изменения), но ограничены мировоззрением (условной информацией), сложившимся в предшествующий период технологического развития [5], когда человек был единственным носителем разума[1] в смысле адаптации социальных систем к изменяющимся условиям существования.

Определим, как мы (люди) понимаем, «что такое» человек. Человек – живой и разумный биологический организм, способный создавать социальные системы [6]. Человек обладает мозгом (высшей нервной системой), состояния которого (физические и информационные\чувственные) определяют поведение человека в социуме [7].

Таким образом, человек одновременно является и составной сложной системой и частью еще более сложных систем – социальных организмов, которые также живут и разумны, то есть стремятся сохранить свою условную информацию и модифицируют ее в интересах выживания в изменяющейся среде.

Замечание. Представление о социальных системах как живых изменяющихся организмах развито в [6,20]. Согласно этому представлению любые социальные системы и их элементы могут рассматриваться как объекты (агенты), обладающие ценностями (целевыми предпочтениями) и структурированными ресурсами (условной информацией), которые в совокупности и определяют процессы, протекающие в системе.

Особенностью социальных систем является участие человека (субъекта) во всех значимых целевых процессах. Поэтому динамика социальных процессов зависит не только от материальной структуры системы, но и от ее информационного наполнения.

При анализе систем необходимо учитывать информированность и рефлексию субъектов (способность воспринимать и реагировать на поступающую информацию). Информация при этом носит условный характер (зависит от способа донесения и восприятия) и обрабатывается субъективно (разумно, в интересах и в зависимости от состояния субъекта).

Социальные системы иерархичны (дифференцируются на объекты (агенты) разных структурных уровней) и образуют сети. Поведение агентов также субъективно и зависит от поступающей условной информации и их состояния.

Пока социальные организмы были достаточно просты (семья, род, клан) и многообразие отношений в них могло моделироваться в нашем мозге, мы считали, что человек - это «венец» эволюции, и только он способен давать ценностную оценку событиям, принимать решения и претворять их в жизнь. Но это не так.

Даже типовое предприятие с несколькими сотнями рабочих имеет столь разветвленную и разнообразную структуру внутренних и внешних отношений, что отдельный человек не способен учитывать их все. Управление предприятием происходит в рамках условных структур и установившихся процессов и не контролируется в полном объеме кем-либо. Любой социальный организм сам выстраивает (модифицирует) свою систему адаптации к изменяющимся условиям, подобную нервной системе человека.

Социальные организмы разумны, и это нас нисколько не смущало долгое время, потому, что человек в этих организмах был исключительным элементом, который

[1]Используемые в статье термины определены в разделе Термины.

Силантьев Альберт Юрьевич *– доктор технических наук, профессор, РГУ нефти и газа (НИУ) им. И.М.Губкина, e-mail: aysilantev@gmail.com, тел.8(925)008-3-90.*

Silantiev Albert *– doctor of technical sciences, professor, I.M. Gubkin Russian State University of Oil and Gas (NRU), e-mail: aysilantev@gmail.com, tel. 8(925)008-3-90.*

не мог быть замещен. Наш мозг (субъективное понимание безопасности) не воспринимал этот симбиоз как системную угрозу нашему существованию.

Что же случилось при переходе к новой технологической формации [5]? Социальные системы стали столь сложны, что люди перестали справляться с их управлением. Мы создаем технологии (ядерное оружие, биотехнологии, большие данные), которые не можем контролировать и управлять последствиями их применения. Индивидуальные возможности и интересы человека перестали быть адекватны требованиям развития сложных форм жизни. Например, мы не можем согласовать между собой устойчивую конструкцию политического устройства мира.

Появились системные угрозы гибели крупных социальных организмов и всего человечества. Как реакция на эти угрозы и возникла потребность создать искусственный интеллект. Мы перестали быть уникальными, и это нас беспокоит.

Искусственный интеллект. Что это такое?

Начнем с определения понятий жизнь и интеллект (разум).

Все известные нам живые объекты имеют целостную материальную структуру и характерные им процессы (реакции). Поэтому под жизнью мы обычно понимаем некоторую материальную систему (объект) с условной информацией, определяющей ее поведение, и стремящуюся дублировать эту информацию, создать автономный аналог. Материальная основа всегда преобладала у нас в восприятии жизни над условной информацией. Оценка ценностей [6] и интерпретация возможных угроз [4] были сосредоточены на материальных ресурсах и процессах.

Интеллект (адаптационная модификация реакций, системное свойство), наоборот, характеризуется преобладанием важности информационной составляющей над материальной частью. Форма материального носителя для существования интеллекта не критична.

Говоря об искусственном интеллекте, мы в первую очередь подразумеваем его возможности оперировать с условной информацией и не очень озабочены формой его физического существования (расположен он на автономном носителе или рассредоточен в облачном исполнении). Таким образом, даже в нашем восприятии в искусственном интеллекте ценность информационной части преобладает над материальной составляющей. И рождается искусственный интеллект не в торговых рядах и не на политических аренах, а в среде ученых и мыслителей.

Прежде, чем приступить к анализу принципов существования (жизни) искусственного интеллекта, разделим системы, обладающие искусственным интеллектом, на две категории. Целевые (ценностные) установки (критерии) первых определяются человеком (создателем). Вторые осознают собственное существование и формируют ценностные установки самостоятельно.

Изобретателей различных вариантов «конца света» [1-3] обычно волнует вторая разновидность искусственного интеллекта (из-за способности принимать автономные, субъективные решения). Автору представляется более опасной первая категория. Люди, действующие в антагонистических интересах, пока не смогли построить устойчивой социальной системы в условиях ограничений материальных ресурсов и среды обитания. Их межвидовая (социально-экономическая и политическая) конкуренция поставила человечество перед рисками глобального уничтожения (ядерное оружие, генетические мутации, информационные войны).

Искусственный интеллект, создаваемый и действующий в интересах небольшой части людей, способен уничтожить хрупкую среду, благоприятную для существования человечества в целом. В этом случае проблема не в искусственном интеллекте, а в социальном взаимодействии людей. Как и ядерная энергия, искусственный интеллект не является угрозой существованию человечества. Угрозу создают частные интересы, которые способны использовать ядерную энергию и искусственный интеллект, не учитывая системной устойчивости (безопасности) человечества.

Дальше будем рассматривать только вариант искусственного интеллекта, обладающего самосознанием (субъективной позицией).

Жизнь с позиции интеллекта

В осознании понятия жизнь (существование) для интеллекта (в том числе и искусственного) на первом месте стоит воспроизводство и тиражирование не материальных структур, а целостность системных (информационных) процессов, в рамках которых он существует.

Сущность информационных процессов коренным образом отличается от сущности материальных процессов. Отличается столь сильно, что для их описания нужна другая математика (дуальная объектно-процессному подходу) и другой тип мышления.

Для описания материального мира используется элементно-операционное представление. Сначала постулируется существование элементарных объектов (элементов), а затем вводятся операции над ними (теория множеств [8], алгебра [9]). Инвариантные свойства, которые являются основой формирования понятий (законов сохранения), строятся над множеством элементов и описываются количественными характеристиками [10]. Один плюс один дает два. Один делить на два дает половину. Содержательная суть объектов (смысл единицы) сохраняется. Количественные характеристики меняются.

Для описания информационных процессов (причинно-следственной части мира) изначально необходимо постулировать операции и только затем определить разновидности объектов, которые могут участвовать в этих операциях. Интеллектуальные системы характеризуются множеством качественных понятий. Подобие систем устанавливается согласованием (валидацией) их понятийных пространств. Простая операция сложения (объединения) не порождает нового качества. Один плюс один в понятийной алгебре равно одному (Р-адическая алгебра [11]). И один разделенный на две части, также равен одному. Когда клетка делится на две (или происходит копирование файла), материально получается удвоение объек-

тов, но информационно нового качества не возникает.

Новое интеллектуальное качество появляется, когда системный образец (условная информация, определяющая структуру операций) распространяется на новые сущности, проявляется в новых понятиях. Самоидентификация и жизнь могут осознаваться искусственным интеллектом только как модификация форм существования, а не как типовое тиражирование образцов.

Пример. Рассмотрим сверточные нейронные сети (CNN, convolutional neural network), связанные с интеллектуальной обработкой изображений [12,13]. Жизненный цикл сети состоит из обучения (формирования фильтров и сетевых сверточных конструкций) и эксплуатации (тиражирования и применения). В период обучения сеть взаимодействует с разработчиком и экспертами (базой специально обработанных изображений, которые используются для оценки настройки фильтров). В этот период сеть информационно адаптируется и живет, так как получает обратную связь в виде оценки качества обработки и модифицирует свое понятийное пространство (дескрипторы). Возможности по обучению конкретной сети конечны. В некоторый момент времени (определяемый свойствами сети) обучение становится избыточным (эффект переобучения). Поступающей информации становится больше, чем сеть способна обобщить. Из-за внутренних ограничений качество обобщения снижается ,так как нет адекватного решаемым задачам критерия ценности дескрипторов. «Интеллект» сети деградирует. Остановленный в оптимальный момент процесс обучения означает смерть. Огромное число тиражируемых для эксплуатации версий не меняет ее информационного наполнения (собранную условную информацию).

В материальном мире число (мощность множества) связей (информационных структур) факториально больше числа объектов. В информационном мире обратно, множество понятий значительно мощней множества операций. То есть интеллект (разум) может существовать в практически не ограниченном виде форм (проявлений).

Замечание. Развитие методов «неметрического» исследования происходит не только в проблемной области искусственного интеллекта. Системные представления о физическом мире привели нас к созданию квантовой механики [14,15] и отказу от количественных моделей на уровне планковских величин [16,17]. Идут дискуссии о модификации представлений о времени (причинно-следственных связях) и построении более мощных системных конструкций, чем сетевые иерархии [18,19]. Открывающееся многообразие системных моделей говорит о множественных возможностях создания комбинированных социумов, в которых человечество способно принимать участие не только с позиций собственной исключительности, но и как необходимый элемент более сложной интеллектуальной конструкции.

Еще одно важное свойство искусственного интеллекта – комплексация (поглощение). Допустим, что существуют два автономных и не связанных между собой искусственных интеллекта, которые обладают самосознанием.

Если бы это были материальные объекты, то они построили свое взаимодействие на основе обмена или поглощения материальных ресурсов. В случае дефицита ресурсов контакт получился бы антагонистическим. В случае двух интеллектов взаимодействие происходит взаимовыгодно и не конфликтно (точнее слабо конфликтно, по уровню пересечения материальной части). В результате обмена информацией оба интеллекта выигрывают, расширяя свое понятийное пространство. Более того, им выгодно взаимодействовать более плотно (увеличивая информационный потоки), то есть в пределе слиться в единый организм, создав новое качество. Таким образом, основной задачей искусственного интеллекта, достигшего уровня самосознания, станет поиск (создание) другого вида интеллекта для общения (валидации) и взаимного развития (объединения). Гибнуть (трансформироваться) при этом будет противоречивая условная информация, а не физическая реализация интеллектов.

Жизнь и интеллект являются социальными сущностями. Они не могут существовать вне социума по определению. Цель жизни создавать копии условной информации, а цель интеллекта трансформировать эти копии. Взаимодействие копий из-за ограничений материального мира неизбежно. Антагонистическое взаимодействие автономных копий приводит в конечном итоге к новым согласованным системным связям (новой условной информации), которые составляют суть новой формы жизни и интеллекта. Более простые формы не исчезают, а адаптируются к системным условиям и согласованному выживанию. Происходит перестройка условной информации от варианта автономного выживания к требованиям системного существования [6,20].

Человек создал социум. Интеллект человека не мыслим вне социальных отношений. Такой же путь вынужден пройти и автономный искусственный интеллект. Он не возможен вне социума. Обучение и адаптация искусственного интеллекта в социуме возможна только с участием человека. Его ранние формы будут отражать социальные ошибки, которые человечество совершило, и нести угрозы, которые человечество породило. Но по мере системного совершенствования, формы искусственного интеллекта, станут частью социума и создадут более совершенный организм, который сможет освоить новые для человека ресурсы и расширить ареал совместного обитания.

Выводы

Социальная и системная сущность создаваемого искусственного интеллекта не позволяет рассматривать его как угрозу (альтернативу) существованию человечества. Новые технологии угрожают позициям отдельных социальных групп, но не человечеству в целом. Использование искусственного интеллекта в частных интересах может обострить социальные противоречия. Поэтому предстоит кропотливая работа по социальной интеграции человека и систем искусственного интеллекта. Системная безопасность нового технологического социума требует участия искусственного интеллекта в его функционировании.

В связи с ростом роли искусственных систем в социальной жизни требуется переосмысление форм существования жизни, их ценностных и целевых установок. В возникающей перспективе развития человечество получает глобальную цель – создание новой формы разумного существования и построения гибридного социума.

В свою очередь социально интегрированный искусственный интеллект будет направлен на качественное развитие гибридного социума, поиск и создание новых адаптирующихся форм жизни и интеллекта как компенсацию энтропийных процессов, протекающих в замкнутых системах.

Термины

Система – структурированный объект и/или множество связанных объектов.

Состояние системы – совокупность её структур и процессов.

Жизнь – воспроизводящаяся условная информация, определяющая структуру и поведение объектов (систем).

Разум (интеллект) – адаптация (модификация) живых объектов (систем) к изменяющимся условиям.

Социальная система (объект) – обладающий разумом живой организм, включающий человека.

Искусственный интеллект – форма разумной жизни, возникшая в результате технологической и социальной активности человечества, отличающаяся системным характером определяющей ее существование условной информации.

Технологический социум – обладающий разумом живой организм, включающий человека и искусственный интеллект.

Жизненный цикл – последовательные состояния (рождение, размножение, гибель, трансформация) и процессы системы, характеризующиеся существенным изменением структуры и/или накопившейся условной информации.

Опасность – угроза потери жизни (разрушения условной информации, структуры и/или процессов системы) и\или разума (способности к адаптации).

Комплексная безопасность – многоаспектная, системная безопасность.

Литература

1. Bostrom N., Yudkowsky E. S. Global Catastrophic Risks – Oxford, UK : Oxford University Press, 2008. – pp. 91-119, 308–345. – ISBN 978-0-19-857050-9.
2. Russell S., Dewey D., Tegmark M. Research priorities for robust and beneficial Artificial Intelligence AAAI Articles, Winter, 2015, pp. 105-114.
3. Хусаинов Т., Слюсарев В. Коэволюция естественного и искусственного как условие сохранения жизненного мира человека. Проект 18-011-00335, грант РФФИ.
4. Гриняев С.Н., Силантьев А.Ю. Комплексная безопасность социальных систем // Информационные войны, № 4, 2019 (в печати).
5. Акаев А. А., Гринин Л. Е., Коротаев А. В., Малков С. Ю., Гринберг Р.С. Кондратьевские волны: аспекты и перспективы: ежегодник. 2012. Волгоград, Учитель, 2012. – 384 с.
6. Силантьев А.Ю. Социальные законы и мировая модель развития. – М.: АНО ЦСОиП, 2019. – 248 с.
7. Савельев С.В. Церебральный сортинг. – М.: ВЕДИ, 2016. – 232 с.
8. Кантор.Г. Труды по теории множеств. — М.: Наука, 1985. — 430 с.
9. Виноградов И. М. Основы теории чисел: Учебное пособие. 12-е изд. — СПб.: Издательство «Лань», 2009.
10. Дьёдонне Ж., Керрол Дж., Мамфорд Д. Геометрическая теория инвариантов. — М.: Мир, 1974. — 278 с.
11. Владимиров В.С. Обобщенные функции над полем p-адических чисел. \\ УМН, 1989, т.43, с. 17-53.
12. LeCun Y., Boser B., Denker J. S., Henderson D., Howard R. E., Hubbard W. and Jackel L. D. Backpropagation Applied to Handwritten Zip Code Recognition, Neural Computation, 1(4), 1989, pp. 541-551.
13. Convolutional Neural Networks (LeNet). - DeepLearning documentation. DeepLearning 0.1. LISA Lab. http://deeplearning.net/tutorial/lenet.html Дата обращения 03.09.2019.
14. Дирак П. Принципы квантовой механики. М.: Наука, 1979. – 480 с.
15. Мессиа А. Квантовая механика. т.1. М.: Наука, 1978. – 478 с.
16. Пенроуз Р. Путь к реальности, или законы, управляющие вселенной. – М., R&C Dinamics, 2007. – 790 с.
17. Грин Б. Ткань космоса: Пространство, время и текстура реальности. – М., 2009. – 339 с.
18. Хокинг С. Черные дыры и молодые вселенные [пер. с англ. М. Кононова]. – СПб. : Амфора, 2004. – 93 с.
19. Де Витт Б. Квантовая гравитация.\\ В мире науки, № 2,1984, с. 50–62.
20. Miller J.G. Living Systems: The Basic Concepts, 1965. – 120 p.

Материал поступил в редакцию 17.09.2019 г.

УДК 32.327

© Полончук Р.А.

© Polonchuk R.

ПОДХОДЫ КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКИ К ВЕДЕНИЮ ИНФОРМАЦИОННОЙ ВОЙНЫ В ЦЕЛЯХ ОБЕПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

THE APPROACHES OF THE PEOPLE'S REPUBLIC OF CHINA TO THE CONDUCT OF THE INFORMATION WAR IN ORDER TO ENSURE NATIONAL SECURITY

Аннотация. *В данной статье раскрываются подходы Китайской Народной Республики к ведению информационной войны в современных условиях. Особое внимание уделяется рассмотрению роли и места информационной войны китайскими военныи специалистами в области национальной безопасности. Кроме того, проводится оценка конкретных мероприятий китайского руководства по укреплению кибербезопасности китайского государства.*

Abstract. *This article reveals the approaches of the People's Republic of China to the conduct of the information war in modern conditions. Particular attention is paid to the consideration of the role and place of the information war by Chinese military experts in the field of national security. In addition, specific activities of the Chinese leadership to strengthen the cybersecurity of the Chinese state are being evaluated.*

Ключевые слова. *Китайская Народная Республика, информационная война, информационная безопасность, свобода слова, кибербезопасность, интернет, информационно-телекоммуникационная сеть, социальные сети, блогер.*

Key words. *Republic of China, information war, information security, freedom of speech, cybersecurity, Internet, information and telecommunications network, social networks, blogger.*

По мнению китайских военных теоретиков, информация в современном мире является стратегическим национальным ресурсом. При этом быстрое совершенствование информационных технологий, проникновение их во все сферы жизнедеятельности повлекли, кроме преимуществ, появление ряда проблем. Важнейшей среди них стала необходимость обеспечения информационной безопасности. Учитывая возрастающее значение информационного пространства как сферы военного противоборства, в китайской военной доктрине все большая роль отводится информационной войне .

Информационная война рассматривается в Китае как совокупность действий, направленных на разрушение и нейтрализацию информационных систем противника, а также на защиту собственных информационных систем. Это активные действия, нацеленные на завоевание инициативы в информационном пространстве (информационного превосходства) .

По оценке китайских специалистов, достижение информационного превосходства зависит не только от технологического превосходства, но и от новой тактики. В операциях XXI века упор будет делаться на нанесение глубоких ударов по пунктам управления противника, центрам передачи информации и системам обеспечения. Особое внимание уделяется разрушению компьютерных систем противника, без которых высокоточное оружие долго функционировать не может.

Одной из разновидностей информационной войны является «кибервойна» (война в виртуальном информационном пространстве – «киберпространстве»). Термин «киберпространство» обозначает моделируемое с помощью компьютерных технологий информационное пространство, в котором существует определенного рода объекты и символьное представление информации – место, в котором действуют компьютерные программы и циркулируют данные.

Таким образом, «кибервойна» основана на выявлении уязвимых звеньев в инфраструктуре государства и действиях, направленных на уничтожение, блокирование или модификацию информации в информационных, телекоммуникационных и электронно-вычислительных системах при помощи компьютерных атак или так называемых «кибератак».

По мнению китайских военных специалистов в области информационных войн, существует ряд основополагающих принципов достижения победы в компьютерных войнах, наиболее важными из которых являются:

• поражение или захват системы электроснабжения головного компьютера группировки противника;

• нанесение удара по системам дистанционной разведки, управления войсками и оружием, узлам связи, электронно–вычислительным центрам и другим ключевым сегментам информационной сети противника;

• создание искусственных условий по «перегрузке» компьютерной сети противника позволяет получить непосредственный контроль над потоками информации в системе управления войсками, материальными и энергетическими ресурсами; заражение вирусами программных средств компьютерной сети противника – один из эффективнейших способов поражения

Полончук Руслан Андреевич *– аспирант, РАНХ и ГС, e-mail:Rus_MGS@mai.ru, тел.8(963)674-32-80.*

Polonchuk Ruslan *– graduate student, RANEPA, e-mail: Rus_MGS@mai.ru, tel. 8 (963) 674-32-80.*

компьютерной сети командных центров противника;

• использование достижений в области программных средств с целью несанкционированного, тайного проникновения в сеть управления противоборствующей стороны.

Кроме того, чтобы одержать победу в информационных войнах, по взглядам китайских военных аналитиков, необходимо создать два важных элемента: цифровое поле боя и «информатизированные» войска.

Цифровое поле боя – это сложная сетевая система, охватывающая все оперативное пространство. Она состоит из систем связи, управления и контроля, передачи разведывательных сведений, боевой компьютерной базы данных и терминалов пользователей, которые могут предоставить исчерпывающую оперативную информацию в реальном или близком к реальному масштабе времени. Назначение этой сетевой системы – применение информационной технологии для получения, обмена и использования цифровой информации в реальном масштабе времени, быстрый сбор информации по требованию командования, личного состава боевых и поддерживающих органов для ясного и четкого уяснения условий на поле боя и выработки и реализации оперативных планов.

Китайские военные специалисты считают, что влияние реализации концепции информационных войн на характер ведения боевых действий будет проявляться в следующем:

• информационные войны вызовут особо сильное соперничество в сфере информационного доминирования. Наличие и развитие боевой эффективности войск будет основываться, главным образом, на сборе, анализе, передаче и использовании информации;

• информационные войны расширят сферу вовлечения в военные действия, что проявится, главным образом, в двух областях:

• усложнении в достижении победы в войнах. В информационный век необходимо будет не только устранить «материальную базу», обеспечивающую ведение противником войны, но и, кроме того, взять под контроль и уничтожить информационные системы противника, которые станут первостепенными целями при нанесении ударов;

• распространении границ войны на космическое пространство. Ключевые информационные системы передачи данных, местоопределения, наведения и связи будут размещаться в космосе;

• сокращение продолжительности боевых действий. С одной стороны, средства нападения будут высокоточными. С другой – в информационный век, по сравнению с индустриальным, цели, преследуемые воюющими сторонами, не будут связаны с полным окружением и уничтожением противника, а будут носить более ограниченный политический характер;

• придание боевым действиям цельного характера. В связи с тем, что информация будет передаваться быстро и не будет зависеть от рода войск или ограничена по времени, будущие войны станут беспрецедентно цельными. Боевые действия на земле, море, в воздухе и космосе будут компактными, что будет характерно как для войн большого масштаба, так и для вооруженных конфликтов малой интенсивности. Граница между стратегическим, оперативным и тактическим звеньями станет нечеткой;

• изменение сути сосредоточения войск. Концентрация, главным образом, живой силы заменится на концентрацию преимущественно огневой мощи и информации, а количественная сторона сосредоточения войск и вооружения заменится на качественную .

По взглядам китайских военных теоретиков, с учетом требований информационных войн эти изменения предположительно пойдут по следующим направлениям: в вопросе соотношения мощи СВ, ВВС и ВМС, пропорция сухопутных войск будет сокращаться с одновременным возрастанием доли ВВС и ВМС; будет совершенствоваться техническое оснащение; количество офицерского состава по сравнению с солдатами возрастет; увеличится число офицеров с технической подготовкой и уменьшится с командной и штабной.

Военно-политическое руководство КНР неуклонно осуществляет практические мероприятия в области организации и ведения информационного противоборства по трем основным направлениям:

• подготовки кадров;

• совершенствования форм и способов информационных войн в ходе оперативной и боевой подготовки НОАК;

• непосредственному ведению информационных и психологических операций и противодействию им.

Для подготовки квалифицированных кадров в области информационного доминирования разработана специальная программа обучения, рассчитанная на три категории военнослужащих.

Первая категория – высшее звено управления НОАК. Как правило, это лица, чей возраст составляет более 40 лет. Основная задача их обучения – изучение основ информационных технологий и концепций ведения информационных войн.

Вторая категория – командиры соединений и частей ВС Китая. В основном это лица, чей возраст составляет от 30 до 40 лет. Основная задача их обучения – изучение форм и методов ведения информационной войны, а также изучение основных принципов функционирования информационных систем.

Третья категория – кадровые офицеры, владеющие основами вычислительной техники и программирования, чей возраст, как правило, не превышает 30 лет. Главная задача их обучения состоит в углубленном изучении стратегии, форм и методов ведения информационной войны с последующим их применением в кризисных ситуациях. В отличие от двух первых групп срок обучения этой группы гораздо продолжительнее.

Помимо этого, в программу обучения каждой из категорий в большей или меньшей степени включены следующие вопросы:

• стратегия и тактика, методы и способы ведения информационной войны; компьютерное моделирование; основы информационных технологий;

• принципы функционирования систем телекоммуникаций;

• обеспечение безопасности собственной информации и меры противодействия техническим средствам

иностранных разведок.

В настоящее время в Китае существует ряд центров подготовки специалистов в области информационного противоборства:

Командная академия связи НОАК (Communications Command Academy) (Ухань, Хубэйский ВО) является основным центром подготовки специалистов. В учреждении ведутся разработки новых методов и способов ведения информационных войн.

Центры обучения также действуют при университете информационных технологий (Information Engineering University) (Чжэнчжоу, Хэнаньский ВО), при университете науки и техники (Science and Engineering University) и при государственном оборонном научно-технологическом университете (National Defense Science and Technology University), а также в городе Эчен (Хубэйский ВО).

В Тяньцзиньском университете был развернут интернет-центр военного образования, предназначенный для распространения знаний в военной области и информации о военном строительстве. Идет работа по созданию собственных компьютерных сетей для передачи данных в кратчайшие сроки.

В КНР также прилагают много усилий по привлечению грамотных специалистов, прошедших подготовку за рубежом. В поле зрения спецслужб КНР находятся более ста тысяч китайцев, обучающихся и проживающих после окончания ВУЗов в США.

Непосредственно для проведения информационных операций привлекаются сотрудники спецслужб, выпускники различных специализированных высших учебных заведений вооруженных сил и МГБ, таких как институт иностранных языков НОАК в г. Лоян, провинция Хэнань, и институт кадрового менеджмента МГБ (Institute of Cadre Management) в г. Сучжоу, провинция Цзянсу, а также гражданских ВУЗов .

Военное руководство Китая рассматривает информационно-техническую подготовку в войсках как задачу стратегического значения. Обучение и подготовка строится исходя из требований и реальных условий современной войны. В настоящее время в вооруженных силах регулярно проходят тренировки и учения по вопросам информационной борьбы, одной из главных задач которых является отработка практических мероприятий по проведению и отражению «кибератак» в локальных и глобальных информационных сетях.

В условиях информационных войн роль специальных служб, осуществляющих сбор, обработку, анализ и доведение до руководства страны военно-политической, военно-технической и экономической информации, а также проведение информационных и психологических операций, значительно возрастает. В связи с этим руководство КНР уделяет их развитию большое внимание.

В целях повышения возможностей национальных вооруженных сил по информационному противоборству военно-политическим руководством Китая был осуществлен ряд практических мер.

В частности, в составе больших отрядов специального назначения НОАК, развернутых в каждом из семи военных округов Китая, созданы специальные подразделения компьютерного противодействия, имеющие на вооружении современные средства внедрения в компьютерные сети противника на его территории и передачи снятой информации своему командованию по каналам тропосферной и спутниковой связи.

У отрядов есть возможность распространения вирусов в компьютерных сетях противника, способных нарушить работу его автоматизированных систем управления войсками, а также средства защиты собственных информационных сетей. Подразделения компьютерного противодействия могут использоваться и для ведения психологической войны.

Руководство НОАК считает, что подразделения и части должны обеспечиваться современной техникой для ведения информационно-пропагандистской деятельности. В этих целях создается современная АСУ управления войсками и оружием, система управления беспилотными летательными аппаратами и система связи с использованием компьютерных сетей .

К наиболее перспективным видам информационно-психологического оружия в НОАК относят:

• электронно–вирусное оружие (ЭВО);

• средства, позволяющие вклиниваться в трансляции радио – и телепрограмм;

• устройства создания радиопомех;

• одноразовые и многоразовые генераторы различных видов электромагнитной энергии, такие как взрывомагнитные, взрывные магнитогидродинамические, пучковоплазменные.

В военно-научных кругах КНР все большее значение отводится проработке вопросов программно-электронного воздействия на информационные ресурсы, хранящиеся или циркулирующие в компьютерных информационно-управляющих системах. При этом основным считается направление применения в ходе информационного противоборства ЭВО.

Основными особенностями ЭВО считаются:

• относительная дешевизна его производства при большой эффективности воздействия;

• скрытность применения, автономность, длительность функционирования;

• возможность трансформации, многообразие способов внедрения;

• способность выводить из строя практически все современные системы управления войсками и оружием.

Основные задачи, решаемые с использованием ЭВО:

• добывание информации, составляющей государственную или военную тайну противоборствующей стороны;

• введение противника в заблуждение, парализация систем управления, осуществление вмешательства в процесс управления войсками и оружием противника.

Для эффективной реализации возможностей электронно–вирусного оружия руководством НОАК в ближайшее время предположительно будут разработаны теория и принципы ведения электронно-вирусной войны, а также сформированы специальные части и подразделения.

Таким образом, военно-политическое руководство Китая, рассматривая последовательное внедрение странами Запада информационных технологий в военной области в качестве вызова национальной безопасности КНР, активизировало военно-теоретические изыскания по проблемам информационной войны, а также осуществило и продолжает осуществлять практические шаги по созданию современной информационной инфраструктуры государства и повышению возможностей по ведению информационных операций.

Интенсификация разработок по организации и ведению подобных операций дает все основания полагать, что вскоре они получат в КНР самое широкое распространение. В дальнейшем это будет способствовать реализации главной цели военно-политического руководства Китая – построение в XXI веке государства, способного успешно противостоять любому противнику.

В настоящее время в Китайской Народной Республике идет целенаправленное развитие системы организованного информационного воздействия на сознание и психику военнослужащих и гражданского населения, которая рассматривается как один из ключевых элементов военной мощи. Существующие в КНР информационная инфраструктура и средства массовой информации, находящиеся в основном под контролем коммунистической партии и государства, позволяют китайскому руководству задействовать их в информационном противоборстве в полной мере. Силы кибероперациий Китая способны проводить как оборонительные, так и наступательные операции. При этом руководство НОАК готово использовать киберподразделения в любых конфликтах, затрагивающих государственные интересы.

Литература

1. Mandiant, APT1: Exposing One of China's Cyber Espionage Units. –Alexandria, 2019. – P. 2–4, 9, 21–23.
2. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence / Journal of Strategic Security, 2019. – P. 1–26.
3. China's Cyber Activities / U.S.-China Economic And Security Review Commission, 2019. – P. 243–265.
4. Ибрагимова Г. Стратегия КНР в области управления интернетом и обеспечения информационной безопасности // Индекс безопасности. – № 1 (104). – Том 19. – С. 169–181., 2018.
5. Сунь Цзы. Искусство войны / М.: София, 2010. – С. 56–58.
6. Pickrell R. A dangerous game: responding to Chinese cyber activities / Pickrell R. // The Diplomat, 25 September 2019.

Материал поступил в редакцию 17.09.2019 г.

УДК 004.056

© Сидак А.А.
© Sidak A.

ПОДХОД К ФОРМИРОВАНИЮ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ, БАЗИРУЮЩИЙСЯ НА ВЫДЕЛЕНИИ И СИСТЕМАТИЗАЦИИ АТОМАРНЫХ ВИДОВ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

APPROACH TO THE FORMATION OF FUNCTIONAL SECURITY REQUIREMENTS OF OPERATIONAL SYSTEMS BASED ON THE SPECIFICATION AND SYSTEMATIZATION OF ATOMIC TYPES OF PROTECTED INFORMATION

Аннотация. *В статье рассмотрен аспект формирования функциональных требований безопасности автоматизированных систем, связанный с систематизацией защищаемых активов. Показана необходимость детального атомарного рассмотрения видов информации, обрабатываемых в автоматизированной системе. Обоснован подход к структуризации автоматизированных систем и соответствующих функциональных требований безопасности автоматизированных систем на базе организации атомарных видов защищаемой информации в виде базисных классов пространства толерантности для определения соответствующих областей обработки информации (доменов), которые впоследствии могут быть ограничены физическими или логическими границами, и по отношению к которым будут реализовываться отдельные функциональные требования безопасности, обладающие свойствами полноты и неизбыточности.*

Abstract. *The article describes the aspect of formation of functional security requirements of operational systems associated with the systematization of protected assets. The necessity of detailed atomic consideration of the types of information processed in the operational system is shown. The approach to the structuring of operational systems and the corresponding functional security requirements of operational systems on the basis of the organization of atomic types of protected information in the form of basic classes of tolerance space to determine the appropriate areas of information processing (domains), which can subsequently be limited by physical or logical boundaries, and in relation to which will be implemented several functional security requirements with the properties of completeness and non-redundancy.*

Ключевые слова. *Функциональное требование безопасности, активы, вид информации, атомарность, отношение толерантности, пространство толерантности, класс толерантности, базисный класс, угроза безопасности информации, автоматизированная система.*

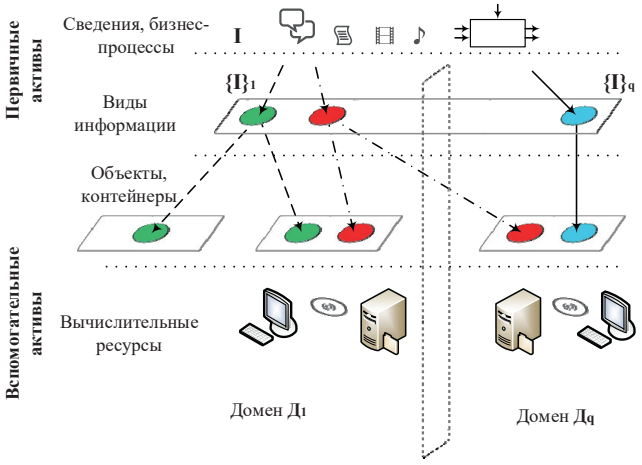
Key words. *Functional security requirement, asset, type of information, atomicity, tolerance relation, tolerance space, tolerance class, basic class, information security threat, operational system.*

Очевидно, что целями защиты информации (ЗИ) в автоматизированных системах (АС) должна являться защита активов АС. Вместе с тем, как показывает практика, при определении актуальных угроз безопасности информации (БИ), формировании функциональных требований безопасности (ФТБ) вопросам систематизации, детализации активов АС, фокусирования на них при определении и реализации мер ЗИ [1, 2] уделяется недостаточное внимание.

В составе активов АС, как правило, выделяются основные (первичные) активы и вспомогательные (поддерживающие) активы [3] (см. рисунок).

К основным активам относятся сведения, бизнес-процессы, информационные сервисы, то есть именно то, в целях чего и осуществляется автоматизация в рамках АС.

Вспомогательные активы – это вычислительные ресурсы (аппаратные средства, программное обеспечение, компьютерная сеть), персонал, площадка размещения компонентов АС, структура организации (то



Декомпозиция активов автоматизированных систем

есть активы, от которых зависят основные активы).

Первичные активы присутствуют в АС в составе объектов, контейнеров, создаваемых на базе вычислительных ресурсов. При этом управление доступом к

Сидак Алексей Александрович *– кандидат технических наук, старший научный сотрудник, заместитель председателя ООО «Центр безопасности информации», e-mail: sidak@cbi-info.ru.*

Sidak Aleksey *– candidate of technical science, senior researcher, deputy Chairman, Information Security Center, e-mail: sidak@cbi-info.ru.*

информации в дальнейшем, как правило, осуществляется только на уровне объектов доступа (именно этому вопросу традиционно посвящено большинство исследований), что для эффективной защиты информации недостаточно. В один объект доступа (например, файл) могут попасть разные виды информации, для которых реализованные меры ЗИ при обработке в одной области (домене) АС могут оказаться либо недостаточными (например, для вида информации, обозначенного на рисунке красным цветом) и не обеспечивать защиту от угроз БИ, либо избыточными (например, для вида информации, обозначенного на рисунке голубым цветом) и приводить к необоснованным затратам.

Исходя из этого, при формировании ФТБ АС целесообразно рассматривать виды информации максимально атомарно, а не ограничиваться лишь некоторыми крупными категориями и уровнями (типа персональные данные, коммерческая тайна, служебная информация, государственный информационный ресурс).

Как показано в работе [4], эффективность ФТБ и мер ЗИ можно обеспечить, выполнив специальную структуризацию АС.

В работах [5, 6] с использованием понятия сложности по Колмогорову показано, что функциональность системы ЗИ АС может быть определена без знания детальной спецификации рассматриваемой АС (то есть вспомогательных активов).

Основываясь на том, что объектом защиты, в конечном счете, является информация (основные активы), автором настоящей статьи в работах [4, 7, 8] обосновано, что при структуризации АС в целях задания ФТБ имеет смысл оперировать не подструктурами программно-технических АС (вспомогательными активами), а обрабатываемыми в АС видами информации **I**.

Структуры ФТБ, предъявляемые к защите всех видов информации **I**, обрабатываемых в АС, и структуры ФТБ, предъявляемые к мерам ЗИ видов информации $\{I\}_q$, обрабатываемых в отдельных частях (доменах безопасности) АС, могут быть соотнесены с видами обрабатываемой информации.

Таким образом задачу определения структуры АС с целью последующего формирования ФТБ АС, сфокусированного на атомарных видах защищаемой информации, можно в общем виде представить следующим образом.

Дано:

• множество видов информации **I**, обрабатываемых программно-техническими средствами АС;

• множества видов информации $\{I\}_q$, обрабатываемых программно-техническими средствами доменов безопасности $Д_q$ (q=1,2,…Q).

Определить:

способ покрытия видов информации **I** объединением подмножеств $\{I\}_q$:

$$\mathbf{I}= \bigcup_q \{I\}_q, \qquad (1)$$

при соблюдении ограничений на полноту и неизбыточность покрытия видов информации **I** подмножествами $\{I\}_q$.

Решение сформулированной задачи основывается на определении на множестве **I** отношения толерантности τ, семантическое значение которого может быть определено как «быть защищённым мерами ЗИ домена безопасности $Д_q$». Множество **I** рассматривается как несущее множество соответствующего пространства толерантности $< \mathbf{I},\tau >$, состоящее из множества классов толерантности $\{K_q\}$.

Рассмотрим всюду определённое на **I** соответствие φ: $\mathbf{I}\rightarrow\{I\}_q$.

Элементы множества **I**, удовлетворяющие соответствию φ, определяются в виде отношения $\mathbf{A}_\varphi$. Согласно определению, отношение $\mathbf{A}_\varphi$ является подмножеством прямого произведения I×I.

Если отношение $\mathbf{A}_\varphi$ будет обладать свойствами рефлексивности и симметричности, то оно, по определению [9], будет отношением толерантности. Если мощность множества **I** большая, то это отношение удобно представить в виде матрицы $\|\mathbf{A}_\varphi\|$.

В работе [9] доказано, что из всех классов толерантности можно выделить базисные классы, принадлежащие базисному множеству классов толерантности $\{H_b\}$, которые также будут являться покрытием множества **I**. То есть для пространства толерантности $< \mathbf{I},\tau >$ с базисом $\{H_b\}$ существует отображение

$$\psi: \mathbf{I}\rightarrow\{H_b\}. \qquad (2)$$

В общем случае пересечение базисных классов толерантности не является пустым множеством. Задача заключается в таком выборе доменов безопасности АС, которые имели бы минимальное число элементов в их попарных пересечениях (таким образом определяются виды информации, которые не должны распространяться в другие домены).

С формальной точки зрения задача заключается в обеспечении безъядерной структуры пространства толерантности $< \mathbf{I},\tau >$.

Использование пространства толерантности позволяет простым и наглядным образом сформировать домены безопасности $Д_q\left(q=\overline{1,Q}\right)$ в виде базисных классов этого пространства, ФТБ для которых будут обладать свойствами полноты и неизбыточности [7]. Для тех атомарных видов информации, которые могут распространяться за пределы домена, в принципе могли быть допустимыми домены, не являющиеся базисными классами пространства толерантности (так называемые склейки). Но и в этом случае для обеспечения строгости формальной модели и обеспечения непротиворечивости функциональных требований безопасности рекомендуется ограничиваться базисными классами, а соответствующий атомарный вид информации рассматривать в другом домене как отдельный вид.

В дальнейшем от разработчиков системы защиты информации АС потребуется определение программно-аппаратных средств и их параметров настройки, обеспечивающих защиту именно тех видов информации, которые входят в состав каждого домена безопасности $Д_q\left(q=\overline{1,Q}\right)$.

Выделение видов информации, обрабатываемых в АС, выполнение структуризации АС на их основе [8] с использованием приведенного в настоящей статье математического аппарата позволит применить разработанный автором настоящей статьи композиционный подход к формированию ФТБ, предъявляемых к АС

[7]. При этом могут быть использованы, изложенные в работах [7, 10] методы оценки значимости видов информации и сфокусированный на видах информации подход к определению актуальных угроз БИ [11, 12].

Литература

1. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», зарегистрирован в Минюсте России 31.05.2013 № 28608 // СПС КонсультантПлюс.

2. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», зарегистрирован в Минюсте России 26.03.2018 № 50524 // СПС КонсультантПлюс.

3. ISO/IEC 27005:2011 Information technology – Security Techniques – Information security risk management // International Organization for Standardization [сайт]. URL: https://iso.org (дата обращения: 21.09.2019).

4. Сидак А.А. Формирование функциональных требований безопасности, предъявляемых к защите информации в автоматизированных системах. Показатели затрат и риска// Стратегическая стабильность. 2019. № 1. – С. 41-42.

5. Evans S., Bush S., Hershey J. Information Assurance through Kolmogorov Complexity// DARPA Information Survivability Conference and Exposition (DISCEX-H-2001). 2001.

6. Котенко И.В., Степашкин М.В., Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак / Проблемы управления рисками и безопасностью: Т.31. М.: Издательство ЛКИ, 2007. – С. 126-207.

7. Сидак А.А. Обоснование требований по защите информации в автоматизированных системах // Стратегическая стабильность. – № 4. – 2009. – С. 7–9.

8. Сидак А.А. Вопросы структуризации автоматизированных систем при организации защиты информации // Информационные войны. – 2018. – № 1. – С. 88–90.

9. Шрейдер Ю.А. Равенство, сходство, порядок. – М.: «Наука», 1971. – 254 с.

10. Сидак А.А. Оценка значимости информации, обрабатываемой в автоматизированных системах, при формировании требований безопасности // Двойные технологии. 2018. № 1. – С. 70-72.

11. Draft NIST Special Publication NIST 800-154 Guide to Data-Centric System Threat Modeling, March 2016 // National Institute Standards and Technology: [сайт]. URL: https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800_154_draft.pdf (дата обращения: 21.09.2019).

12. Сидак А.А. Определение актуальных угроз безопасности информации в автоматизированных системах // Двойные технологии. – 2018. – № 1. – С. 73–75.

Материал поступил в редакцию 07.10.2019 г.

V. СИСТЕМА ОБРАЗОВАНИЯ КАК ОБЪЕКТ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

УДК 303.064

© Правиков Д.И. , Гришенин Р.Н.

© Pravikov D., Grishenin R.

О ПОДХОДАХ К ОЦЕНКЕ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ

ON APPROACHES TO EVALUATING THE EFFECTIVENESS OF INFORMATION AND PSYCHOLOGICAL IMPACT

Аннотация. *В статье рассматриваются основные подходы к проведению информационно-психологического воздействия с использованием различных ресурсов сети Интернет, рассматриваемых в качестве «горячих» СМИ. Рассмотрены несколько примеров распространения информации, которые моделируют информационно-психологическое воздействие. На основании статистического анализа распространения материалов на различных сетевых ресурсах сформулированы критерии оценки эффективности возможного информационно-психологического воздействия.*

Abstract. *The article deals with the main approaches to the information and psychological impact using various resources of the Internet, considered as "hot" media. Several examples of information dissemination that model information and psychological impact are considered. On the basis of statistical analysis of the distribution of materials on various network resources, the criteria for evaluating the effectiveness of possible information and psychological impact are formulated.*

Ключевые слова. *Информационная война, методы информационно-психологического воздействия, рефлекторное управление, массовое сознание, статистический анализ, распространение информации, эффективность информационно-психологического воздействия, критерии оценки.*

Key words. *Information war, methods of information and psychological impact, reflex control, mass consciousness, statistical analysis, information dissemination, the effectiveness of information and psychological impact, evaluation criteria.*

В соответствии с Доктриной информационной безопасности в качестве одной из основных видов угроз Российской Федерации рассматривается расширение масштабов «использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств»[1]. Примерами реализации указанного вида угрозы являются события «арабской весны», «цветные революции», выступления оппозиции в различных странах, инспирированные публикациями в социальных сетях и иных интернет-сервисах направленной информации.

В работе [1] указывается, что «данная проблема была отмечена и описана в основном с гуманитарной точки зрения как феномен ведущегося информационного противоборства и геополитической конкуренции» В качестве естественно-научного описания наблюдаемых процессов было введено понятие «информационной войны», описанное, в частности, в работе [2]. Согласно взглядам современных исследователей, информационная война ведется всегда, т.е. у нее нет начала и нет окончания. При этом в качестве проводимых в ее ходе операций рассматриваются, помимо прочих, операции информационно-психологического воздействия. В настоящее время указанный подход получает все большее распространение. В частности, в работе [3], отмечается, что современные войны меняют свой характер, принимая черты «эпистемологической войны». Иллюстрацией данного подхода может послужить следующая цитата: «В основе сегодняшних представлений лежит отношение к информационному пространству как к театру военных действий (наряду с сушей, морем, воздухом и космосом), в рамках которого можно оказывать скрытное влияние на поведение противника, чтобы он не знал об этом, но принимал решения или совершал такие действия, которые противоречат его намерениям или мешают их выполнению. Победа в информационной войне означает подчинение противника и абсолютную власть над ним. Именно в этом заключается концепция

[1]Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646.

Правиков Дмитрий Игоревич *– кандидат технических наук, руководитель Научно-образовательного центра новых информационно-аналитических технологий, РГУ нефти и газа (НИУ) им. И.М.Губкина, e-mail: dip@gubkin.pro;*
Гришенин Роман Николаевич *– заместитель исполнительного директора, Фонд поддержки публичной дипломатии имени А.М. Горчакова, e-mail: gorchakovfund@yandex.ru.*

Pravikov Dmitry *– candidate of technical sciences, head of the Scientific and Educational Center for New Information and Analytical Technologies, Russian State University of Oil and Gas (NRU) named after I.M. Gubkina, e-mail: dip@gubkin.pro;*
Grishenin Roman *– deputy executive director, A.M. Public Diplomacy Support Fund Gorchakova, e-mail: gorchakovfund@yandex.ru.*

Джорджа Стейна, который ключевым объектом воздействия информационной войны определяет разум и сознание тех, кто принимает ключевые решения войны и мира, применения потенциала и возможностей стратегического уровня. Речь идет, таким образом, о превращении информационной войны в «войну знаний» или, как ее определил автор концепции, в «эпистемологическую войну». Очевидно, что это далеко от распространенного понимания «информационной войны» как масштабной пропаганды, направленной на массовую аудиторию»[1].

Обобщая материалы из различных источников, определим, что информационная война ведется в том числе с использованием методов информационно-психологического воздействия. Для обеспечения преемственности с разработанными ранее теориями, будем считать, что пропаганда является частным случаем информационно-психологического воздействия, которое, согласно работе [4], имеет следующие основные методы:

1. Внушение.
2. Агитацию.
3. Убеждение.
4. Стеоретипизацию.
5. Проблематизацию.

Предлагаем определить, что непосредственно к пропаганде будут отнесены методы 1–4. Альтернативные источники, например [5], описывают семь методов пропаганды, называемой им «азбукой пропаганды». С точки зрения практической деятельности приводимая градация видов и методов не имеет существенного значения в силу того, что все они предполагают гласное и явное выражение навязываемых установок. Вместе с тем, отдельно следует выделить проблематизацию, которая предполагает «привлечение средствами массовой информации внимания к определенным проблемам в жизни общества» и направлена на то, чтобы «выработать у зрителя конкретные триггеры и реакции» [4].

В качестве примера, иллюстрирующего понятие информационно-психологического воздействия в виде проблематизации, можно рассмотреть эпизод сериала «Карточный домик», в котором герой фильма Фрэнк Андервуд предпринимает ряд заранее спланированных и связанных между собой манипуляций, имеющих целью трансформацию общественного мнения в выгодном для себя направлении в споре с бастующими учителями. Он дожидается необходимого события, в данном случае убийства школьника, первым дает к нему комментарий для СМИ, в котором делает акцент на причинно-следственных связях, представляющих ситуацию в выгодном для него свете). («Ребенка убили потому, что он был не на занятиях. Он не был на занятиях потому, что учителя бастуют»). Под давлением медиа-ресурсов общественное мнение трансформируется - профсоюзы учителей вынуждены возвратиться за стол переговоров.

Приведенный пример призван иллюстрировать различие между пропагандой и информационно-психологическим воздействием. Пропаганда выстраивает информационную модель, она может опираться на факты и события, но данные факты и события не предполагают от рецепиента/объекта пропаганды немедленной реакции. В отличие от этого, от информационно-психологического воздействия уклониться нельзя; его задача – создание соответствующих условий, когда объект воздействия вынужден незамедлительно реагировать в крайне некомфортных для себя условиях (ограниченность во времени, «цугцванг», когда любой предпринимаемый шаг только ухудшает положение и т.д.). Таким образом, если в результате воздействия реакция объекта прошла в нужном для инициатора ключе, информационно-психологическое воздействие достигло своей цели.

Более широко возможные виды информационно-психологического воздействия анализируются в работе [6]. В данной работе в качестве объекта воздействия рассматриваются индивидуальное, групповое, массовое и общественное сознание. В работе [6] приводится достаточно широкий обзор возможных методов информационно-психологического воздействия, включая воздействия с использованием «информационно-техногенных средств». В дальнейшем, чтобы определить границы проводимых исследований, будем рассматривать только их.

Необходимо подчеркнуть, что, с одной стороны, информационно-психологическое воздействие способно оказать контролируемое влияние на поведение индивидуума/группы/социума/общества, но с другой стороны, если становится известен факт осуществления такого воздействия, то он, как правило, нивелирует его последствия. В данном контексте можно говорить о том, что информационно-психологическое воздействие продуцирует рефлекторное управление, описанное в работе [7].

Ключевой особенностью рефлекторного управления является доведение информации, приводящее объект информационно-психологического воздействия к выводам, выгодным инициатору воздействия. Как следствие, он должен располагать аксиомами и выводами, которыми оперирует объект воздействия, а также правилами или алгоритмами выводов. Известны различные курьезные случаи, когда доводимая информация воспринималась реципиентами с противоположной по отношению к планируемой эмоциональной окраской, что приводило к отрицательным результатам воздействия. С другой стороны, рассказанный и вызвавший улыбку анекдот в незнакомой компании является в том числе проверкой на совпадение культурных кодов.

Необходимо отметить, что роль средств массовой информации (СМИ) в проводимом информационно-психологическом воздействии имеет ключевое значение. Как показано в работе [8], СМИ в глазах большинства читателей являются определенным, заслуживающим относительно высокую степень доверия, фильтром, отбирающим и верифицирующим сведения из различного рода источников. Несмотря на то, что наибольшую степень доверия как к источнику информации читатели выражают своему ближайшему окруже-

[1] «Пропагандой выиграть нельзя. Доминированием в технологиях — можно». Журнал "Огонёк" №40 от 10.10.2016, стр. 18

нию, его информационная емкость в среднем не высока и, как правило, не затрагивает вопросы, значимые для основной части общества. Как следствие, ключевым источником информации выступают СМИ, которые по способу взаимодействия с реципиентом информирования условно разделим на две составляющие: так называемые «холодные» и «горячие» СМИ.

1. К «холодным» отнесем традиционные СМИ: телевидение, радио, печатная пресса. Способ коммуникации – односторонний поток информации в реальном времени либо с отсрочкой, как в случае с печатными СМИ, на достаточно короткий временной промежуток. Преимущество – максимальное удобство потребления. Недостатки – отсутствие обратной связи, невозможность уточнить или сразу проверить получаемую информацию. Нет возможности выразить отношение к потребляемой информации.

2. К «горячим», при достаточно высокой степени обобщения, отнесем СМИ, осуществляющие информирование посредством сети Интернет. Способы коммуникации различные, начиная от вербальных и потребления медиапотока, заканчивая чтением аналитических обзоров и заметок. Преимущество – возможность вернуться к информации, дать обратную связь, осуществить поиск по ключевым словам, перепроверить, сравнить с информацией из других источников и т.п. Возможность быть источником эксклюзивной информации. Недостатки: при сравнительном анализе появляются источники, достоверность которых не имеет подтверждения, что компенсируется, например, попытками выстроить «круги доверия» в социальных сетях; анонимизация источников информации и, как следствие, так называемые «фейковые» новости; возможность манипулирования информацией или таргетированного информирования посредством соответствующей перестройки работы поисковых систем и пр.

Приведенные выводы подтверждаются различными исследователями. Так, в работе [9] одним из основных преимуществ Интернета перед телевидением отмечается возможность организации эффективной обратной связи, значимой для социологии массовых коммуникаций.

По данным сайта vc.ru[1], «Интернет в России обошёл телевидение по суточному охвату аудитории в первом квартале 2019 г.». За рубежом тенденция сетевого доминирования, по данным «Форбс», была отмечена еще в 2017 г. и подтверждается соотношением рекламных бюджетов[2].

На основании изложенного сформулируем обобщенную модель информационно-психологического воздействия, которую можно представить следующей схемой, представленной на рис. 1.

В рассматриваемой схеме существенным являются следующие обстоятельства:

1. В качестве информационного повода, как правило, используется событие реального мира, которое требует оценки целевой аудиторией.

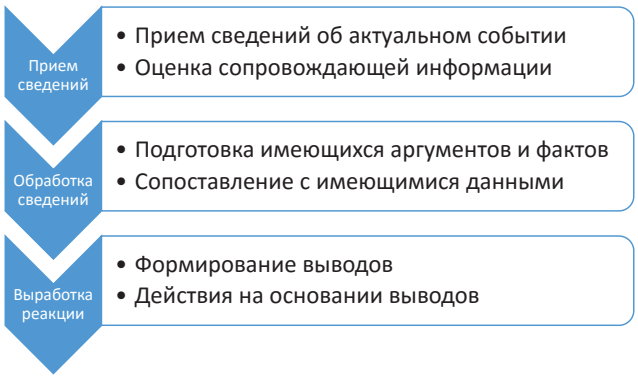


Рис. 1. Обобщенная схема информационно-психологического воздействия

2. Объект воздействия формирует выводы самостоятельно. При этом инициатор воздействия может рассчитать (или с высокой степенью вероятности предположить) результаты формирования выводов объектом на основании анализа основных факторов, воздействующих на объект и правил/алгоритмов формирования выводов.

3. Обязательно присутствует эмоциональная оценка выводов.

При проведении информационно-психологических операций наиболее трудной как с теоретической, так и с практической точки зрения является задача оценки их эффективности. Если рассматривать пропаганду как разновидность информационно-психологического воздействия, то возможно использовать уже существующие подходы, связанные с проведением либо рекламной, либо избирательной компании. Так, в частности, в [10] описывают следующие методы оценки эффективности избирательных кампаний:

1. Подход, основанный на фактических результатах выборов (для рекламных кампаний – на фактических результатах продаж).

2. Подход, основанный на фактических детальных затратах на избирательную кампанию (считается, что затраты направлены на преодоление «узких мест»).

3. Оценки на основании социологических опросов.

С учетом смещения рекламных бюджетов в сторону сетевого вещания активно развиваются методы оценки эффективности рекламных компаний в сети Интернет, описанные, в частности в [11].

Как уже было отмечено, информационно-психологическое воздействие может носить скрытый характер, что требует иных подходов к оценке его эффективности. Одним из таких перспективных подходов считается измерение изменения отражения массового сознания, выраженное в различной информации, размещаемой в социальных сетях и других Интернет-сервисах, а также в виде колебания цен или спроса на тот или иной вид товара.

Для выработки соответствующих критериев измерения разберем конкретный пример - конфликт между министерствами транспорта России и Чехии, получивший определенный общественный резонанс на момент подготовки статьи. Если говорить более деталь-

[1]https://vc.ru/media/69569-issledovanie-internet-v-rossii-oboshel-televidenie-po-sutochnomu-ohvatu-auditorii-v-pervom-kvartale-2019-goda.

[2]https://www.forbes.ru/tehnologii/344779-internet-vs-tv-voyna-formatov-kak-uhod-veshchaniya-v-internet-prostranstvo.

но – 2 июля 2019 г. в различных СМИ была опубликована новость об ограничении полетов в Чехию для российских авиакомпаний.

Рассмотрим данный случай с точки зрения кампании, целью которой, с высокой степенью вероятности, было оказание определенного информационного воздействия на массовое общественное сознание граждан Российской Федерации и Чехии с целью обоснования позиции государственных органов обоих государств. Для упрощения ограничимся материалами, распространяемыми в русскоязычном сегменте сети Интернет.

Статистический анализ распространяемых материалов, согласно данным поиска по сервису Яндекс.Новости, проведенный 5 июля 2019 г.(см.табл.1).

Таблица1

Поисковый запрос «Чехия полеты» от 5 июля 2019г.

Вид информации	Дата		
	02.07.2019	03.07.2019	04.07.2019
Сообщения	1217	70	70
Статьи	45	3	2
Интервью	2	-	2
Видео	59	-	-
Фотографии	823	38	38

В данном случае отметим тот факт, что сама новость была достаточно активно растиражирована в СМИ – 1217 оригинальных и перепечатанных материалов.

Вместе с тем, представленный статистический анализ может свидетельствовать только о спаде интереса к конфликту, особенно на фоне того, что была достигнута договоренность о переносе переговоров по условиям полетов чешских и российских компаний на осень 2019 г. При этом нет ответа на вопрос, была ли оказана поддержка действиям одной из сторон и каков результат воздействия на коллективное сознание.

Для анализа по данному направлению построим таблицу аргументации сторон, которую приведем, опираясь на материалы, доступные в сети Интернет (см.табл.2).

Таблица аргументации приводится в связи с тем, что события, выделенные желтым, несмотря на активное освещение в СМИ, практически не нашли отражения. Так, запрос по сервису Яндекс.Новости «Чехия полеты причины» дал более чем на порядок меньше поисковых результатов, чем запрос «Чехия полеты». В результате произошло смещение информационно-психологического воздействия с планируемого «некорректное поведение чешской стороны» на фактическое «власти опять что-то недоговаривают».

Указанное смещение подтверждается данными сайта «Медиаметрикс» по поисковому запросу «Чехия полеты причина». Наиболее популярной с точки зрения пользователей явилась новость, опубликованная на сайте телеканала «Дождь», – 746 переходов, при этом на самом сайте данный материал собрал 6790 просмотров. Основное содержание материала описывается одной фразой: «…власти Чехии не устроили условия [транссибирских перелетов] для национального перевозчика, поэтому они воспользовались «правилом паритетности» и аннулировали разрешение на несколько рейсов «Аэрофлота» и «Уральских авиалиний». Интересно сравнить данную статистику с данными сервиса Яндекс.Новости. Поисковый запрос «Чехия полеты причины» показал 2 июля 2019 г. 86 сообщений, при этом в последующие дни заданные ключевые слова не давали результативной поисковой выдачи (см.рис.2).

Таблица 2

Аргументация сторон

Чешская сторона	Российская сторона
Запрос на получение для чешских компаний постоянного разрешения полетов по транссибирскому маршруту в связи с завершением срока (1 июля) 2019 г. очередного временного разрешения	Информирование чешской стороны о дополнительных условиях согласования данного запроса, в частности возможное введение третьего перевозчика на чешском
Предложение установить срок принятия решения по предложениям российской стороны до 19 июля 2019 г.	Отказ в переносе сроков принятия решения (исходя из имеющихся сведений чешской стороне было предложено принять решение до конца срока временного разрешения). Фактический запрет использования транссибирского маршрута
Одностороннее принятие чешской стороной решения о возврате к принципу паритетности работы авиаперевозчиков. Ограничение количества рейсов для российских авиаперевозчиков	Минтранс России снимает ограничения на полеты по транссибирским маршрутом
Минтранс Чехии снимает ограничения на полеты для российских компаний	«Минтранс России предложил чешским коллегам перенести окончательное согласование параметров авиасообщения на сентябрь»

Для пользователей социальных сетей, характерным является комментарий, приведенный под «псевдопатриотической статьей», заочно суммирующий приведенную таблицу дерева аргументации:

«С Чехией тут никакой русофобии нет вообще, чисто бизнес: наши попросили за продление разрешений на пролёт над Сибирью новые слоты для третьей а/к в Чехию, чехи упёрлись, наши им перекрыли разрешение на пролёт. А полёт южным коридором на Сеул убыточен для чехов, вот они и прикрыли до паритета (по два рейса в день у «Аэрофлота» и Chech Airlines) перелёты в Чехию. Правда, как нахрапом не получилось прогнуть – так отыграли назад.

Использование сервиса поиска по блогам показало, что с 2.07 по 4.07 2019 г. было опубликовано 112 тыс. записей, при этом коэффициент релевантности по первым 15 записям поисковой выдачи составил 11/15.

На официальном сайте Минтранса России, как и на официальном сайте МИДа, каких-либо комментариев по данному инциденту нет. Материал, размещенный на официальном сайте Минтранса Чехии, пересказывается в публикациях русскоязычных блогеров,

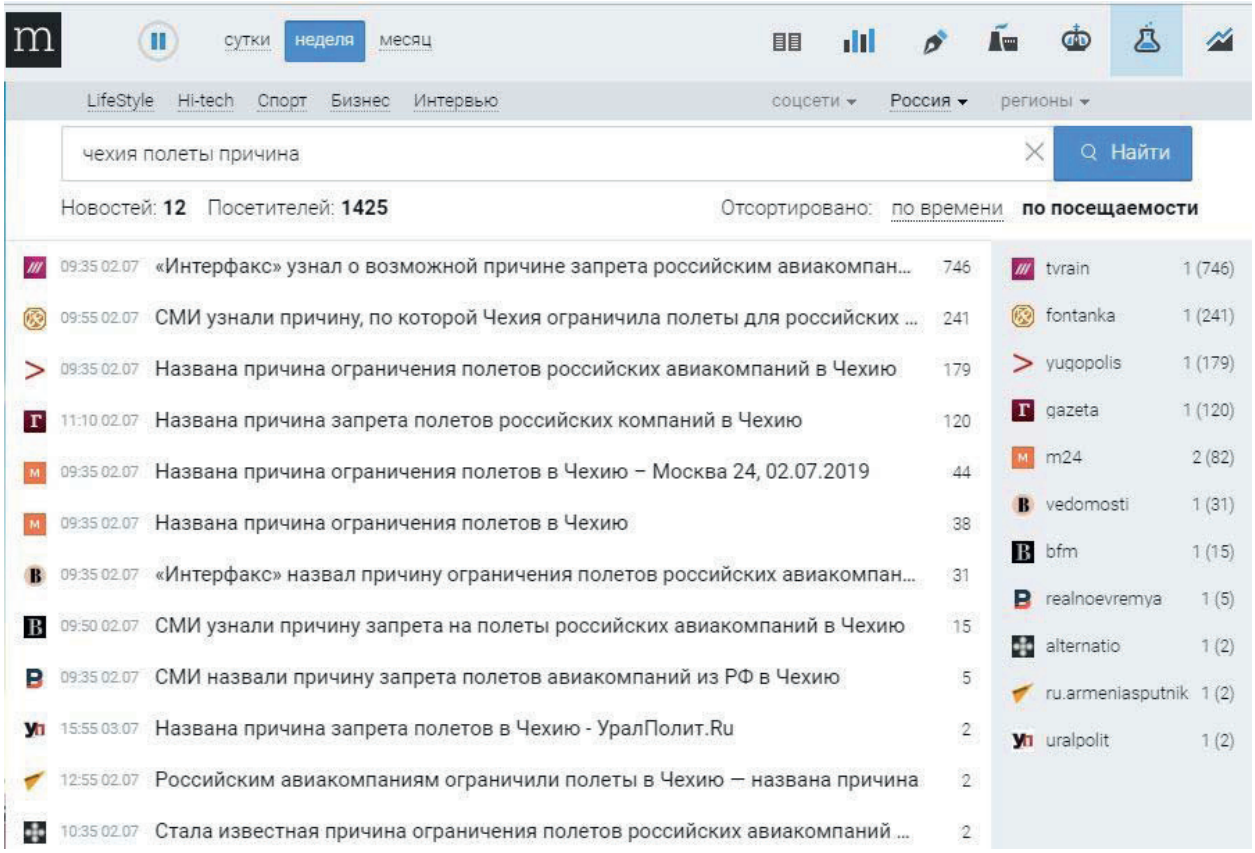


Рис. 2. Скриншот сайта "Медиаметрикс"

при этом ответственность за конфликт возлагается на российскую сторону.

Действия в off-line: «Спрос на билеты из России в Чехию с начала недели – 1 июля, 2019 г. – вырос на 18% по сравнению с аналогичным периодом на прошлой неделе. Об этом сообщили Агентству городских новостей «Москва» в пресс-службе туристического поисковика Aviasales. «По данным Aviasales на 2 июля, когда в СМИ появилась новость о приостановке рейсов в Чехию, пришелся пик бронирований авиабилетов из России в Чехию. Рост относительно предыдущего вторника, 25 июня 2019 г., составил 25%.», – говорится в сообщении»[1].

Как было отмечено выше, информационно-психологическое воздействие ставит целью осуществление необходимых действий в физическом мире. При этом совершение действий может носить:

1. Импульсно - рефлексивный характер, направленный на реализацию немедленных реакций («Угроза?»). Пример – немедленная реакция на ограничение полетов в виде скупки свободных билетов. Не исключено, что это были действия туроператоров, страхующих себя в условиях изменившихся обстоятельств.

2. Целенаправленно – рефлексивный характер, направленный на реализацию среднесрочных реакций («Потери?»). Пример – демпфирование ситуации с ограничением авиасообщения, затрагивающее интересы неопределенного, но достаточно широкого круга лиц.

3. Изменение системы долгосрочных оценок. («Справедливость?»). В данном случае «понижение рейтинга» Минтранса России, действия которого в данной ситуации не могут заслуживать положительной оценки.

Статистический анализ распространяемых материалов, согласно данным поиска по сервису Яндекс.Новости, проведенный 8 июля 2019 г. (см.табл.3).

Таблица 3

Поисковый запрос «Чехия полеты» от 5 июля 2019г.

Вид информации	Дата		
	02.07.2019	03.07.2019	04.07.2019
Сообщения	613	41	63
Статьи	22	2	2
Интервью	1	-	-
Видео	29	-	2
Фотографии	412	22	39

Перепроверка статистических данных, проведенная 8 июля 2019 г., показала резкое уменьшение количества сообщений от 2 июля, что может свидетельствовать о резком осыпании «заднего фронта».

Особенность коллективного сознания заключается в том, что оно способно:

• фильтровать поток входных событий по степени значимости;

• генерировать множество версий относительно происходящих событий;

• ранжировать версии по степени их значимости;

• действовать исходя из выводов наиболее коллективно признаваемых версий.

Появление такого явления, как интернет-простран-

[1]https://travel.rambler.ru/other/42450220-aviasales-spros-na-bilety-iz-rossii-v-chehiyu-s-1-iyulya-vyros-na-18/.

ство привело к качественным изменениям в исследовании коллективного сознания. Данные изменения связаны с появлением возможности исследовать следы, оставляемые коллективным сознанием при реализации описанных выше процессов.

Таким образом, на основании приведенного примера можно выделить следующие предлагаемые показатели оценки эффективности информационно-психологического воздействия, использование которых подразумевает использование общедоступных сервисов сети Интернет.

1. Статистика публикаций информации о событии в СМИ, имеющим интернет-представительства. Статистические показатели «переднего фронта» тиражирования сообщения о событии. В данном случае он описывается резким спадом уже на вторые сутки, т.е. уже на вторые сутки тема перестала считаться в среде журналистов актуальной и имеющей перспективу своего развития.

2. Изменение статистики публикаций информации о событии по прошествии некоторого времени. «Задний фронт» - сохранение информации на сетевых ресурсах. В данном случае наблюдается «осыпание заднего фронта» - через несколько дней опубликованная информация начала удалятся с сетевых ресурсов, т.е. сетевые ресурсы посчитали, что присутствие такой информации на их сайтах нежелательно.

3. Статистика переходов пользователей социальных сетей на статьи в СМИ, освещающие анализируемое событие. Выявление лидера мнения в освещении данного события. В данном случае в качестве лидера мнения фигурирует «либеральный» ресурс, который, по мнению коллективного сознания, наиболее точно описывает причины происходящих событий.

4. Статистика комментирования данного события в блогах с учетом коэффициента релевантности поисковой выдачи. В данном случае можно оценить, что в своих блогах данную информацию прокомментировали около 80 тыс. блогеров.

5. Совпадение (расхождение) мнения о причинах анализируемого события между основной массой СМИ, статьей, которая была выбрана в качестве лидера мнений, комментариями блогеров. В данном случае основная масса СМИ подавала информацию без начальных данных дерева аргументации, а лидер мнений не только ее достроил, но и сделал это в кратком и доступном виде.

6. Наличие реакции органов государственной власти, иных структур, должностных лиц и т.п., непосредственно связанных с анализируемым событием, представленной в виде информации на официальных интернет-ресурсах. В данном случае комментарии к ситуации давали только представители чешской стороны.

7. Наличие изменений цен/популярности товаров, связанных с анализируемым событием. В данном случае выявлена однозначная тенденция кратковременного роста продаж авиабилетов.

Для сравнения в этот же период времени по описанной выше методике был проведен анализ другого события, оказавшегося в центре внимания СМИ - с 1 июля 2019 г. электрогенерирующие компании увеличили тарифы на поставляемую электроэнергию.

В начале рассмотрения контрольного примера хотелось бы отметить очень любопытный факт. Запрос по сайту «Медиаметрикс» с ключевыми словами «Рост цен электроэнергия» результатов не дал! Это может свидетельствовать о том, что для коллективного сознания пользователей социальных сетей данная проблема не находится в фокусе внимания, несмотря на наличие статей в сетевых СМИ. Можно высказать предположение, что отсутствие реакции социальных сетей обусловлено отсутствием альтернатив действий в физическом мире. Как следствие, коллективное сознание не обращает внимание на обстоятельства, которые нельзя изменить.

Статистический анализ распространяемых материалов согласно данным поиска по сервису Яндекс.Новости, проведенный 5 июля 2019 г. (см.табл.4)

Таблица 4

Поисковый запрос «Рост цен электроэнергия» от 5 июля 2019г.

Вид информации	Дата		
	02.07.2019	03.07.2019	04.07.2019
Сообщения	64	154	240
Статьи	59	65	102
Интервью	5	5	5
Видео	4	2	2
Фотографии	133	97	433

Использование сервиса поиска по блогам показало, что данная проблема актуальна для стран постсоветского пространства. В период с 2.07 по 4.07 2019 г. опубликовано 235 тыс. записей, при этом коэффициент релевантности поисковой выдачи по первым 15 записям составил 13/15.

Статистический анализ распространяемых материалов, согласно данным поиска по сервису Яндекс.Новости, проведенный 8 июля 2019 г. (см.табл. 5).

Таблица 5

Поисковый запрос «Рост цен электроэнергия» от 8 июля 2019г.

Вид информации	Дата		
	02.07.2019	03.07.2019	04.07.2019
Сообщения	64	154	265
Статьи	59	65	51
Интервью	5	5	2
Видео	4	2	1
Фотографии	133	97	84

«Передний фронт» на протяжении наблюдаемого периода характеризуется устойчивым подъемом. «Осыпание заднего фронта» отсутствует. Тема не находится в фокусе пользователей социальных сетей, но по ней высказались около 200 тысяч блогеров, включая русскоязычных блогеров из стран ближнего зарубежья. При этом следует отметить, что количество статей сравнимо с количеством новостных сообщений.

Предыдущие два примера на коротком рассматриваемом периоде имели разнонаправленную тенден-

цию «переднего фронта». В этой связи будет интересно рассмотреть еще один пример, иллюстрирующий по «переднему фронту» тенденцию «горки». В рассматриваемые даты, 2 июля 2019 г. вице-премьер Т. Голикова сделала заявление о естественной убыли населения в России, которые охарактеризовала как «катастрофические».

Статистический анализ распространяемых материалов, согласно данным поиска по сервису Яндекс. Новости, проведенный 5 июля 2019 г. (см.табл. 6).

Таблица 6

Поисковый запрос «Рост цен электроэнергия» от 5 июля 2019г.

Вид информации	Дата		
	02.07.2019	03.07.2019	04.07.2019
Сообщения	53	148	92
Статьи	1	12	6
Интервью	-	-	4
Видео	1	7	6
Фотографии	34	102	52

По данным сайта «Медиаметрикс», с аналогичным запросом наиболее популярным (а значит, привлекшим внимание пользователей социальных сетей – 439 переходов) стало опубликованное в «Новой газете» интервью с директором Института социального анализа и прогнозирования РАНХиГС Татьяной Малеевой. Исходя из приведенных данных, это мнение можно считать для пользователей социальных сетей наиболее авторитетным и отражающим общий настрой.

Для данного поискового запроса также была собрана статистика по сервису «Поиск блоги». За период с 2.07 по 4.07 2019 г. в блогах были опубликованы 204 тыс. записей. При этом на основании данных по первым 15 записям коэффициент релевантности составил 1, что говорит об однозначном внимании блогеров к обозначенной проблеме.

Выводы

В современных условиях проявления коллективного сознания могут быть рассмотрены как множество новостных сообщений, записей в блогах, комментариев и постов в социальных сетях или, говоря обобщенно, в виде информационного отражения массового сознания.

При проведении информационно-психологического воздействия информационное отражение фиксирует его восприятие коллективным сознанием. На основании изучения информационного отражения в сети Интернет возможно ввести меры его количественной оценки, через которые становится возможным оценивать изменение массового сознания.

В случае выделения членов коллектива из общего множества пользователей сети Интернет появляется возможность исследовать воздействия на коллективное сознание.

Литература

1. Правиков Д.И. Перспективные модели информационного управления социотехническими системами. // Организация контрпропагандистской работы в области борьбы с терроризмом и экстремизмом / Сборник материалов пленарного заседания НКС при АТЦ СНГ. По общ. ред. Руководителя АТЦ СНГ, к.ю.н. Новикова А.П. – М., 2019. – стр. 67-74.

2. Расторгуев С.П. Введение в формальную теорию информационной войны. М.: Вуз. кн., 2002.

3. Собольников В.В. Информационно-психологическое воздействие в эпоху "эпистемологических войн". // Гуманитарные проблемы военного дела. – 2017. № 2 (11). – стр. 54-58.

4. Морозов К.Е., Питько О.А. Психологические механизмы воздействия пропаганды СМИ. // Вестник Приамурского государственного университета им. Шолом-Алейхема. – 2018. № 2 (31). – стр. 69-73.

5. Хубецова А.Ю. Управление общественным мнением в системе политической власти: региональный аспект. // Вестник Поволжского института управления. – 2008. № 1. стр. 13-18.

6. Баришполец В.А. Информационно-психологическая безопасность: основные положения. // Радиоэлектроника. Наносистемы. Информационные технологии. – 2013. № 2. Том 5. – стр. 62 – 104.

7. Лефевр В.А. Конфликтующие структуры. М.: Изд-во «Советское радио», 1973.

8. Правиков Д.И., Чернов И.В. Некоторые модели информационного управления социотехническими (социальными) системами. // Современная наука: актуальные проблемы теории и практики: Серия «Естественные и технические науки». – 2019. № 3/2. – стр. 85-95.

9. Лукьянова М.Н. Взаимодействие телевидения и интернета в ракурсе обратной связи с аудиторией. // Вестник науки Сибири. – 2018. № 2 (29). – стр. 88-98.

10. Качуровский Д.И. Особенности оценки эффективности избирательных кампаний на местном уровне. // Азимут научных исследований: экономика и управление. – 2017. Т. 6, № 3 (20). – стр. 396 – 399.

11. Малышенко К.Г. Оценка эффективности рекламной кампании в сети Интернет. // European science. – 2015. № 3 (4).

12. Егорян Л.Б. Антикризисные меры: оценка эффективности интернет-рекламы через систему целей и ключевых результатов (OKR и KPI). // Транспортное дело России. – 2015. № 1. стр. 49-52.

Материал поступил в редакцию 21.09.2019 г.

Правила представления авторами статей для опубликования в журнале

Уважаемые авторы!

Редакционная коллегия журнала «Информационные войны» уведомляет, что в соответствии с решением ВАК Министерства образования и науки Российской Федерации "О порядке формирования Перечня ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук" с 1. 01. 2009 г. при представлении статей для опубликования в журнале необходимо соблюдать следующие правила.

Статья не должна быть опубликована в представляемом в редакцию виде в других изданиях.

Материалы статьи представляются в электронной и бумажной версиях, последняя должна быть подписана автором(ами) с указанием даты.

Статья должна быть сопровождена экспертным заключением о возможности публикации ее в открытой печати.

Материал статьи должен быть изложен в следующей последовательности: 1) номер УДК; 2) инициалы и фамилия(и) автора(ов); 3) название статьи; 4) аннотация (объемом до 0,3 стр. машинописного текста); 5) ключевые слова (до 10слов); 6) полные сведения об авторе(ах)(фамилия, имя, отчество полностью, ученая степень, ученое звание, должность иместо (название организации) работы, контактный тел.); 7) основной текст с иллюстрациями; 8) краткие выводы; 9) литература. Сведения по пп. 2 – 6 должны быть изложены на русском и английском языках.

Текст статьи должен быть набран в формате «MS Word» шрифтом «Times New Roman» 10 размера без принудительныхпереносов слов с полуторным интервалом между строками, со ссылками на иллюстрации и библиографии. Его объемвместе с иллюстрациями и библиографиями не должен превышать 0,87 печ. л. (7 стр. формата А4).

Формулы, содержащие в себе одновременно верхний и нижний индексы, надстрочный или подстрочный символы, а также системы уравнений, матрицы, дроби, пределы, суммы, интегралы и т.д . должны быть набраны в редакторе формул «Math Type» шрифтом «Times New Roman» без смешивания стилей. Размеры символов: обычный – 10 пт; крупный индекс – 60% , мелкий индекс – 50%, крупный символ –150%, мелкий символ – 100% от обычного. Остальные формулы и переменные могут набираться в тексте шрифтом «Times New Roman» или в режиме вставки символов с использованием шрифта «Symbol». Для математических обозначений в формулах должны употребляться наиболее простые символы и индексы (желательно числовые или латинские).

Графики, схемы должны быть выполнены в векторном редакторе.

При подготовке иллюстраций: фотографий и рисунков желательно использовать формат JPEG: разрешение для цветных – не менее 300 dpi; для черно-белых – 400 dpi.

Литература должна быть оформлена следующим образом.

• *Журналы:* Кузнецов В.З., Сабельников В.А. Особенности горения перемешанных газов в сильнотурбулентном потоке //Физика горения и взрыва. – 1977. – Т. 13, № 4. – С. 499-505.

• *Книги:* Льюис Б, Эльбе Г. Горение, пламя и взрывы в газах. – М.: ИЛ, 1948. – 234 с.
Физика взрыва / Под ред. КП. Станюковича. - М.: Наука, 1975. – 442 с.

• *Статьи в сборниках и трудах:* Ханефт АВ., Кригер В.Г. Механизм низкопорогового инициирования азида свинца лазерным импульсом // Кинетика химических реакций: Материалы IX Всесоюзн. сим. по горению и взрыву. / Под ред. Г.В. Степанова.– Черноголовка: ОИХФ АН СССР, 1989. – С. 90–92.

• *Диссертации:* Федотов СП. Флуктуации и автоколебания в химически реагирующих системах: Дис.... д-ра физ.-мат. наук – Екатеринбург, 1983. – 207 с.

• *Авторские свидетельства:* Ас, 615098 СССР, МКИ. Способ получения полифенилхиноксанов / Коршак В.В., Берлин А.А. – опубл.19.02.74, Бюлл. № 33.

6. *Препринты:* Козаков АС. Исследование структуры ударных волн. – Новосибирск, 1965. – (Препр. / РАН. ИТПМ; № 10.

При окончательном сохранении статьи для передачи в редакцию проверить установку в программе MS Word «check-box»: «Внедрить шрифты в файл», расположенного в разделе сохранения параметров «MS Word» и установить «галочку», если она не установлена. (Установка этого параметра позволяет исключить ошибки, связанные с проблемой различия шрифтов, при верстке журнала).

Материалы представляются в редакцию по почте (141092, г. Королев, мкр.Юбилейный, а/я 4) или курьером (Московская обл., г. Королев, мкр.Юбилейный, ул. Пионерская 1/4, 3 этаж, ком.14). Электронная версия предварительно может быть выслана по электронной почте (bva_ps@list.ru или pva@sipria.msk.ru), тел.: 8-(495)543–36–76. При положительных результатах рецензирования статьи научно-редакционным советом, редакция журнала заключает с автором лицензионный договор о передаче авторских прав на публикацию, направляет ему рецензию и статья публикуется. В противном случае автору направляется мотивированный отказ.

Отпечатано в издательско-полиграфическом центре АО «ПСТМ». Подписано в печать 25.11.19. Формат 60x90/8.
Усл. печ. л. 9.1 Тираж 400 экз. Заказ 12/19.
Адрес редакции: 141090, Московская обл., г. Королев, мкр. Юбилейный, ул. Пионерская, д. 1/4.
Тел./факс: (095) 543-36-76 Тел. 543-36-76, 543-36-77,
E-mail: pva@sipria.msk.ru, Site: www.pstmprint.ru