Artificial societies. 2013-2021

ISSN 2077-5180

URL - http://artsoc.jes.su

Issue 1-4 Volume 11. 2016

Information and Networking Influence: Reality of Ourdays

Irina Bobkova

Abstract

The use of information networking technologies, various methods of influence is becoming the most important problem in the conditions of Internet expansion. The general problems of informational influence on the modern persons in the context of economic security of Russia and psychological safety of Russians are formulated.

Keywords list (en): information and network effects, realities of our time

Date of publication: 29.12.2016

Citation link:

Bobkova I. Information and Networking Influence: Reality of Ourdays // Artificial societies. – 2016. – V. 11. – Issue 1-4 [Electronic resource]. URL: https://artsoc.jes.su/s207751800000005-4-3/ (circulation date: 08.05.2021).

1 Информационное воздействие возникло не в XX веке. Оно существовало с давних времен. Выражалось это воздействие в создании мифов и дезинформации. Больших успехов в этой области добились древние спартанцы, Чингисхан, Великобритания в Первой мировой войне, большевики при подготовке Октябрьской социалистической революции, Геббельс при аннексии Австрии [Губанов,1]. Однако на совершенно новый уровень информационное влияние вывели политические и военные структуры США. США разработали и испытали в реальных войнах целостную концепцию современных информационных технологий [Бобкова, 2]: в Корее и Вьетнаме прошла обкатка концепции информационного воздействия; 1990-е гг. – «Буря в пустыне» и операция на Гаити, когда специалисты группы психологических операций СВ США проводили целенаправленную обработку каждой отдельной группы населения [9]; расчленение Югославии, где «Голос Америки» транслировался прямо с самолетов ВВС США. В 2000-е гг. основная борьба велась против Ирана. 2010е гг. – это революции в Египте, Тунисе,

Ливии, Сирии. Затем центр борьбы переместился на Украину, с целью отделить ее от России.

2 Одна из причин такого внимания Пентагона и руководства США к технологиям информационного воздействия – установка на максимальное сохранение жизни американским солдатам, участвующим в вооруженных конфликтах, в которых заинтересованы или принимают участие США, см. также табл.1.

3 Таблица 1. Потери США в войнах, в которых они участвовали в XVIII-XXI вв. *Источник:* [DeBruyne, 3]

Военный конфликт	**Период**	**Число пострадавших**	**Число убитых**	**% летальных исходов**
Революционные войны	1775-1783	10623	4435	42
Война 1812 г.	1812-1815	6765	2260	33
Мексиканская война	1846-1848	5885	1733	29
Гражданская война	1861-865	422295	140414	33
Испано-американская война	1898	2047	385	19
Первая мировая война	1917-1918	257404	53402	21
Вторая мировая война	1941-1945	963403	291557	30
Корейская война	1950-1953	137025	33741	25
Вьетнамская война	1961-1973	200727	47424	24
Война в Персидском заливе	1990-1991	614	147	24
Война в Ираке и Афганистане	2004-2013	10369	1004	10

4 Информационное воздействие в отношении России:

5 1-й этап – после Второй Мировой войны; СССР - «Империя Зла», а капиталистические страны – «Империя Добра»; *результат* – советских людей боялись и ненавидели, ожидая ядерного удара по городам США;

6 2-й этап – 1970-е гг. – подмена советских моральных ценностей капиталистическими; *результат* - изменение сознания советской молодежи;

7 3-й этап – 1980-е гг. – в 1979 г. СССР был вынужден вмешаться в гражданскую войну в Афганистане, идущую между афганским правительством и проанглийской исламской оппозицией; *результат:* весь мир осуждает действия СССР, бойкотирует Олимпиаду-1980;

8 4-й этап – распад СССР в 1991 г., информационная пропаганда, работа с национальными элитами стран бывшего СССР, СМИ, использование экономических трудностей для информационно - психологической обработки населения; информационная война против России во время Чеченской войны и Грузино-Осетинского конфликта; *результат:* поддержка чеченских террористов, режима Саакашвили, несмотря на выводы комиссии ОБСЕ об агрессии именно грузинских властей;

9 5-й этап – с конца 2013 г. – Украина, Россия, Евросоюз – учебное пособие по проведению информационной войны, от психологической обработки до провоцирования военного конфликта; *результат* –Украина разваливается на глазах, тысячи жертв на Донбассе, Европу лихорадит. В процессе операции в Сирии, РФ столкнулась с оголтелой пропагандой, которой мы не знали даже во времена холодной войны, причем со стороны как западной прессы, так и Интернета. Огромное количество форумов, часто украинского происхождения посвящено ужасам действий Асада и российского контингента – видеоролики, фото, комментарии. Часть СМИ занимается откровенным враньем, публикуя фотошопные фото, компании поприличней, например BBC, подтасовкой фактов и умалчиванием. Каков

будет результат этих акций – покажет время.

10 **Информационно-сетевое воздействие (ИСВ).** Дадим несколько определений по информационному воздействию [Петров, 4].

11 1. Информационно-сетевое воздействие – использование информационно-сетевых технологий для психологического, технического, военного и др. воздействия на индивидуума, группу лиц или государство.

12 2. Информационное противоборство – это комплексное взаимное информационное воздействие сторон друг на друга, которое способно привести к принятию благоприятных для инициатора воздействия решений либо парализовать информационную инфраструктуру противника (радиоэлектронная борьба, действия на психологическом и мировоззренческом уровнях, дезинформация, внушение и т. п.).

13 3. Информационная война – это захват сырьевых, энергетических и других ресурсов чужой страны путём нанесения ущерба информации, информационным процессам и системам противника при одновременной защите собственной информации и информационных систем, распространения ложной информации и манипуляции сознанием населения, устраняющей способность этого населения к сопротивлению. Целью является закрепление большей части стратегически важных ресурсов страны за геополитическим агрессором, причем передача этих ресурсов осуществляется элитой страны-жертвы «добровольно».

14 Целями ИСВ являются [Шеремет,5]:

15 • политическое и военное руководство страны (подкуп главных лиц государства, алкоголь, наркотики, женщины, семья и т.п.);

16 • системы жизнеобеспечения (электронные и технические диверсии);

17 • население (взлом паролей, идентификационных номеров, банковских счетов, конфиденциальных данных, дезинформация, использование информационно-коммуникативных и манипулятивных методов обработки населения, образование и воспитание);

18 • вооруженные силы (электронное вмешательство в процессы командования и управления военными объектами и системами, «штабная война», вывод из строя сетей военных коммуникаций, сбор развединформации).

19 Обстоятельства, способствующие успеху ИСВ:

20 • создание глобальной мировой информационной сферы – развитие инфраструктуры Интернета, экспоненциальный рост Интернет-устройств, совершенствование телекоммуникаций;

21 • рост количества технических объектов, использующих Интернет – военные системы и оборудование, энергетика и транспортные сети, телекоммуникации и информация, системы управления государством, финансовая система;

22 • рост влияния инфосферы на сознание индивидуумов, различных социальных групп, всего населения страны – реклама в Интернете, социальные сети, компьютерные игры для манипулирования сознанием молодежи.

23 Влияние этих обстоятельств в ближайшем будущем будет усиливаться в связи с ростом пользователей Интернета в мире (см. табл.2).

24 **Таблица 2.**Рост числа пользователей Интернет (прогноз на конец 2016 г.). (по данным [Cisco Visual Networking Index,6])

Параметр	**Прогнозные данные**
IP-трафик	1,3 зетабайт (1,3*1012 Gb)
Число интернет-соединений	18,9 млрд (2,5 соединения на каждого жителя Земли)
Рост числа пользователей	3,4 млрд (45% населения Земли)
Частные интернет-пользователи	2,3 млрд
Пользователи устройств мобильного доступа в интернет	4,5 млрд
Число пользователей Рунета	69,3 млн чел (53% населения)
Численность российских пользователей социальных сетей	34,5 млн чел (24,4% населения)
WiFi соединения	50% интернет-трафика
Выход в сеть не реже 1 раза в месяц	2330 млн чел

25 Аналитики компании Gartner вообще прогнозируют увеличение числа пользователей до 6,8 млрд, на 30% больше, чем в 2015 г.(Hogan, 10). Самые высокие темпы роста интернет-трафика в 2014-16 гг. наблюдались у быстро развивающихся стран: Индии - 62%, Бразилии и ЮАР – по 53%. Численность пользователей наиболее популярных социальных сетей Facebook, YouTube примерног по 1,5 млрд, ВКонтакте свыше 300 млн. А наибольший темп роста пользователей соцсетей наблюдался в Индии 37,4 %, Индонезии 28.7% и Мексике 21,1%.

26 Одним из показателей влияния Интернета на население является перемещение рекламы из ТВ-пространства в Интернет (табл.3).

27 **Таблица 3**. Рост расходов на рекламу в интернете по сравнению с ТВ в РФ (по данным [Коммерсантъ, 7])

Параметр	2012	2013	2014
Реклама контекстная, мдрд руб	48,06	51,6	…
В % к предыдушему году	128	107	…
Реклама на ТВ, млрд руб	143,26	156,2	151,3
В % к предыдушему году	118	109	97

28 В 2010-х гг. усилилось информационное противостояние между Востоком и Западом, христианским и исламским миром, США и Россией, Китаем. Ираном и другими странами, проводящими самостоятельную политику. Оно проходило по нескольким направлениям:

29 • перенос агрессии в информационно - сетевое измерение, провоцирование социальных столкновений;

30 • резкое возрастание роли телеканалов в разжигании конфликтов (наиболее успешные - CNN и канал «Аль-Джазира»);

31 • усиление влияния западной идеологии на традиционные общества ($385 млн - затраты США на помощь повстанцам в Сирии, $2700 млн - на войну в Ливии в 2011 г. ; $432 млн - затраты Франции на войну в Ливии в 2011 г.; $385 млн - затраты Великобритании на войну в Ливии в 2011 г.; на протяжении всего конфликта в Ливии поступала противоречивая и заведомо ложная информация, которую распространяли каналы Аль-Джазира и Аль-Арабия, британский BBC, американский CNN, французские France24, France-TV) (Тьерри Мейсан, Политологический центр Reseau Voltaire).

32 **Информационные технологии в военном деле.** Еще два – три года назад многие отрицали сам факт существования информационно-сетевого воздействия в военных целях.

Военные эксперты включают в это понятие штабную войну, электронную, психотропную, информационно-психологическую и т. д. Основные боевые действия ведутся в социокультурной сфере: образование, СМИ, наука, охрана природы, органы управления государством. Информационная война предполагает проведение мероприятий, направленных против систем управления, против компьютерных и информационных сетей и систем противника.

33 Министерство обороны (МО) США выделяет на информационную безопасность более $10 млрд в год на следующие цели:

34 защита информационных систем - объединенная рабочая группа по защите компьютерных сетей, объединенное космическое командование ВС США, национальный центр защиты инфраструктуры;

35 реагирование на компьютерные инциденты- рабочие группы ВВС США, сухопутных войск, ВМС США, транспортного агентства МО США, АНБ;

36 ведение ИВ - центр информационной войны ВВС США, центр СВ по разработке мероприятий по ИВ, центр разработки мероприятия по ИВ ВМС США, центр ИВ ВМС США, центр технологии ИВ;

37 расследование компьютерных преступлений - отдел специальных расследований ВВС США, директорат криминальных расследований армии США, военная разведка СВ, служба криминальных расследований ВМС США, служба криминальных расследований МО США;

38 проведение операций в информационных сетях - центр сетевых операций ВВС США, компьютерное и телекоммуникационное командование ВМС США, центр безопасности операций в глобальных сетях;

39 разведка - разведывательные управления объединенного штаба, МО США (около 6 тыс. человек, бюджет $1 млрд), ВВС США;

40 обеспечение - объединенный центр борьбы с системами управления, центр совместного использования электромагнитного спектра, компьютерная судебная лаборатория МО США, агентство перспективных оборонных исследований, пункт управления совместными операциями по единому информационному обеспечению деятельности подразделений американской армии и др.;

41 другие организации МО - Национальное управление по аэронавтике и исследованию космического пространства, объединенный центр оборонных исследований, рабочая группа университета Карнеги Меллона и др.

42 Кроме МО, вопросами информационной войны в США занимаются и другие структуры, в частности АНБ (штат более 20 тыс. человек; бюджет свыше $3 млрд), ЦРУ (более 15 тыс.; около $3 млрд), ФБР (свыше 25 тыс.; $3 млрд), отделения ФБР по борьбе с компьютерными преступлениями, президентская комиссия по защите национальной инфраструктуры, университеты, фонды, исследовательские фирмы и другие организации. Совокупные расходы США на ИСВ составляют около $50 млрд, а суммарные затраты на разработки в области ИВ в мире в настоящее время превышают $120 млрд в год [Гриняев, 8].

43 Новейшие проекты Пентагона в области ИСВ осуществляют[Стельмашенко, 9]:

44 объединение киберкомандования (Unified U.S. Cyber Command), основано в 2010 г. на базе двух структур Пентагона – Объединенной группы по операциям в глобальной сети и Объединенного командования структурных компонентов сетевых боевых действий (ОКК –

главный специалист по информационным войнам);

45 Surrogate Subjugation - системы автоматизированного мониторинга социальных сетей, форумов и чатом (цель – влияние на аудиторию, для чего создается профиль пользователя, в котором представлена специально подобранная информация, в том числе указаны интересы, увлечения и политико-экономические взгляды; данные подбираются таким образом, чтобы оказывать влияние на других участников дискуссий; этот «пользователь» благодаря своей легенде и комментариям формирует отношение других людей к себе);

46 SMISC (Social Media in Strategic Communication) – занимается мониторингом политических дискуссий и с помощью анализа выявляет пропаганду со стороны противников (враждебной нации или группы людей; его задача – революционный прорыв в области сетевых технологий, их использование для контроля и управление общественным мнением);

47 Broadcast Monitoring System (BMS) и Web Monitoring System (WMS) - системы мониторинга телерадиовещания и сети Интернет, разрабатывались специально для Пентагона компанией BBN Technologies (BBN); системы обрабатывают информацию на 75 языках мира в автоматическом режиме и на основе полученной информации составляют обзоры блогов, форумов и чатов);

48 CWOC (Cyberspace Warfare Operations Capabilities) – для уничтожения, влияния и искажения компьютерных сетей и центров управления противников (при помощи атак на серверы, заражении и взлома операционных систем и других сетевых устройств, установления контроля над киберпространством (бюджет проекта - $10 млн.).

49 **Американские программы по социальным медиа в стратегических коммуникациях (SMISC)**

50 СМИ – это политическая власть. Поэтому перед властью постоянно стоит проблема альтернативных СМИ, а в наши дни еще и свободного от контроля Интернета (из-за журналистских расследований срываются сроки военных и политических кампаний, становятся общим достоянием преступления солдат). Несмотря на официальную пропаганду, независимые информационные кампании не позволяют сделать необходимую "правду" достаточно эффективной. Поэтому в разных странах мира идет активная работа по разработке и совершенствованию инструментария ведения информационных войн.

51 В частности, с 2011 г. в Пентагоне разрабатывается новая система SMISC, которая будет отслеживать все политические дискуссии и уста-навливать, является ли дискуссия случайной или это пропагандистская операция. На те участки соцсетей, где появляется позиция, противоположная американским интересам, будут направлены дополнительные усилия для отстаивания интересов и поднятия престижа США.

52 Такие организации как DARPA (Department of Arpanet) – департамент МО США, отвечающий за все передовые технологии, IARPA (Intelligence Advanced Research Projects Activity - Агентство передовых разведывательных исследовательских проектов) и ARL имеют все возможности для распространения влияния США через Сеть (разрабатываются программы, позволяющие автоматизировать процесс мониторинга, подготовки и проведения активных мероприятий) [11].

53 **Экономическая подоплека информационной войны против России и других стран.** Экономическая выгода от информационной войны против России - бесплатные поставки ресурсов, огромный российский рынок, согласие по внешнеполитическим вопросам, устранение конкурента на многих высокотехнологичных рынках, поток образованных мигрантов, одностороннее разоружение России, выплата финансовой дани, процентов по

кредитам. В 1991-2011 гг. США выделили на «демократизацию России» только официально $9 млрд. (фактически - $19.6 млрд): 3.8 млрд долл. - российским агентам через USAID, финансируемую Госдепартаментом США, 6.7 млрд - через «другие активные программы грантов» (Other Active Grants Programs), 3.9 млрд. - через Department of Defense Security Assistance, 247 млн - через другие госпрограммы помощи (Other State Assistance), 4.95 млрд - «экономическая помощь», «борьба с наркотиками», «помощь в развитии», «борьба с терроризмом» и др.

54 В декабре 2013 г. официальный представитель Государственного департамента США В. Нуланд призналась, что на аналогичную демократизацию Украины было выделено $5 млрд. Ущерб от этой деятельности пока подсчитать трудно, но зато уже есть цифры по ущербу от ИСВ США в других странах, переживших конфликты в последние годы. Например, в Ливии - 50000 пострадавших, в т.ч. 6000 пропавших без вести, до 3000 погибших, до 20000 раненых, до 750 тыс беженцев, бюджетные потери – $14 млрд, замороженные счета – $145 млрд, потери нефтяной отрасли - $50 млрд, в т.ч. $20 млрд от неэкспорта и т.д.

55 Можно сформулировать основные угрозы экономической безопасности России в результате ИСВ: увеличение дифференциации населения и повышение уровня бедности, в т.ч. за счет инфляции, безработицы, свертывания соцпрограмм; возможный дефицит на некоторые товары, задержка заработной платы; падение рубля, цен на нефть, ухудшение положения в банковском секторе (опасность санкций для ВТБ, Сбербанка, Газпромбанка и др.), блокирование счетов, проблемы с расчетами в валюте и т.д.; возрастание неравномерности экономического развития регионов в связи с введением жестких санкций; криминализация общества из-за роста безработицы, преступлений в среде мигрантов, где безработица будет на порядок выше.

56 **Выводы.** Главные законы РФ по обеспечению информационной безопасности страны - Указ Президента РФ от 12.05.2009 «О стратегии национальной безопасности Российской Федерации до 2020 г.» и Закон «О защите критической информационной структуры РФ». Однако, национальный план информационной защиты должен постоянно корректироваться, что потребует все большего увеличения средств. По каждой из угроз должны быть выработаны свои стратегии защиты. Вопросами информационной безопасности должны заниматься не только военные и технические, но и экономические научные подразделения. Экономические интересы, лежащие в основе политических решений, затраты на развитии телекоммуникационных магистралей, на контрпропаганду и развитие систем контроля, защита собственных сетей от киберугроз, ликвидация экономических последствий ИСВ и многие другие вопросы должны стать предметом отдельного экономического анализа.

Информационно-сетевое воздействие – реалии нашего времени

Бобкова Ирина Александровна

Аннотация

Использование информационно-сетевых технологий, различных методов влияния становится все более острой проблемой в условиях повсеместного внедрения Интернета. В работе сформулированы основные проблемы информационного воздействия на современного человека в контексте экономической безопасности России и психологической безопасности россиян.

Ключевые слова: информационно сетевое воздействие, реалии нашего времени

Дата публикации: 29.12.2016

Ссылка для цитирования:

Бобкова И. А. Информационно-сетевое воздействие – реалии нашего времени // Искусственные общества. – 2016. – Т. 11. – Выпуск 1-4 [Электронный ресурс]. URL: https://artsoc.jes.su/s207751800000005-4-3/ (дата обращения: 08.05.2021).
